IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

BLIX INC.,	)	
	)	
Plaintiff,	)	
	)	
v.	)	C.A. No. 19-1869-LPS
	)	
APPLE INC.,	)	**JURY TRIAL DEMANDED**
	)	
Defendant.	)	

AMENDED COMPLAINT

Plaintiff Blix Inc. ("Blix" or "Plaintiff") hereby demands a jury trial and alleges the following against Defendant Apple Inc. ("Apple" or "Defendant"):

INTRODUCTION

1. Plaintiff Blix Inc. is an industry-leading provider of software solutions and innovating messaging products. Ben Volach, co-founder of Blix, has been a pioneer in online messaging for almost 20 years. In 1999 Mr. Volach co-founded Followap—a leading provider of mobile messaging products. Followap enabled advanced interoperable mobile messaging products and presence-enhanced services. It eventually served more than 200 million subscribers before being acquired by NewStar for roughly $140 million.

2. After Followap's success, Mr. Volach continued to develop innovative messaging products. Mr. Volach knew that as electronic communication became more prevalent, privacy would become a growing concern. Mr. Volach had a vision for an easy-to-use communication system that would give individuals manageable addresses to control their privacy and manage interactions. Using Mr. Volach's ideas, companies and individuals could use manageable *public* addresses while keeping their *private* address information private. The system Mr. Volach

envisioned was a revolutionary step forward, allowing electronic communication without widespread dissemination of private address information.

3. Mr. Volach captured his vision in a patent application, and the U.S. Patent and Trademark Office ("USPTO") agreed Mr. Volach's ideas were patentable innovations. Mr. Volach received U.S. Patent No. 9,749,284 ("the '284 patent") on August 29, 2017.

4. Mr. Volach used these ideas to develop BlueMail—a beautifully designed, universal email application capable of managing an unlimited number of mail accounts from various providers while enabling personalization across multiple email accounts.

5. BlueMail was first released in 2014 and quickly achieved success on multiple platforms. It became one of the top three email applications on Android, with over one million downloads and more than 500,000 ratings and reviews (91% of which are "highly satisfied"). It achieved similar success on the iOS "App Store" in terms of user satisfaction. BlueMail was named as one of the "Coolest Must Have Phone Apps" for 2017 by NBC's Today Show.

6. In August 2018, Mr. Volach added innovative anonymous messaging features to BlueMail, adding a "Share Email" feature to facilitate private and easy-to-manage communications options. BlueMail's new "Share Email" feature allows parties to communicate using manageable *public* interaction addresses, without revealing their *private* interaction addresses. This new feature was a major step towards implementing the visionary ideas in Mr. Volach's patent.

7. Not long after Mr. Volach's team unveiled BlueMail's innovative anonymous communication options, Apple took Mr. Volach's pioneering ideas—without permission, payment, or credit—and used those ideas in Apple's own products.

8. In June 2019 Apple announced a new "Sign In With Apple" service for fast, easy-to-use, private messaging. At a worldwide conference for Apple software developers, Apple's Senior Vice President of Software Engineering Craig Federighi described a system for controlled interactions, using manageable public interaction addresses and private interaction addresses. This new system received thunderous applause. But during the presentation, Apple never acknowledged that this idea for manageable interaction addresses was *already* being used in other software—Mr. Volach's popular BlueMail software.

9. Not only did Apple steal BlueMail's pioneering anonymous messaging capabilities—days later, Apple *removed* BlueMail from the MacOS App Store, to prevent Mr. Volach's software from readily reaching consumers and competing with Apple's own products. This unlawfully leveraged Apple's monopoly over MacOS's App Store (Apple's closed system for MacOS application distribution) to extend, maintain, and protect from competition Apple's monopoly power in the market for MacOS mail clients (including Apple's pre-installation of its own proprietary Apple Mail software on each MacOS device Apple sells).

10. Apple's theft of Mr. Volach's patented ideas, days before Apple threw Mr. Volach's very successful software product out of Apple's "App Store" marketplace, caused tremendous harm to Blix. For years Mr. Volach has been preparing to release software that extends BlueMail's use of secure and private messaging, to make full use of Mr. Volach's vision in his '284 patent. For that reason, Mr. Volach co-founded Blix—a successor company to BlueMail—to take the next step in BlueMail's evolution. But Apple's theft of Mr. Volach's patented technology is now crippling the long-planned rollout of new features in BlueMail and Blix.

11. Apple's unexplained and unjustified refusal to give consumers access to competing software products in the App Store is a threat to Blix's success. The BlueMail client for Mac has been ejected from the App Store, making it inaccessible to consumers who use MacOS and who would benefit from BlueMail's innovative features. Apple's conduct leaves consumers with fewer choices when selecting an email application for MacOS.

12. Consumers also suffer from Apple's pattern of stealing great ideas Apple sees in the App Store. Apple frequently takes other companies' innovative features, adds those ideas to Apple's own software products without permission, and then either ejects the original third-party application from the App Store (as it did with Blix's software) or causes the third-party software developer to close its doors entirely. This pattern of behavior is well documented. *See, e.g.,* Washington Post, *How Apple Uses Its App Store To Copy The Best Ideas* (Sept. 15, 2019) (attached as Ex 1) ("Developers have come to accept that, without warning, Apple can make their work obsolete by announcing a new app or feature that uses or incorporates their ideas. Some apps have simply buckled under the pressure, in some cases shutting down. They generally don't sue Apple because of the difficulty and expense in fighting the tech giant—and the consequences they might face from being dependent on the platform… Apple's creation of apps imitating ones that already exist on its platform, aided by market data it collects from them, could be harming competition and hurting innovation.").

13. Apple's monopoly over app distribution forecloses competition and harms consumers—reducing consumer choice, discouraging third-party software developers from investing in future innovative products, and reducing competition among applications. Apple's anticompetitive use of its App Store harms competition through multiple mechanisms, as described herein – including unfair denials of access to the App Store, efforts to leverage its App

Store dominance into dominance in other markets, and activities (such as intellectual property theft based on its analysis of App Store submissions) that increase rivals' costs, discourage entry by new software developers, unfairly tilt the playing field in Apple's favor, and make it harder for companies like Blix to compete.

14. Blix, and its BlueMail product, are the latest in Apple's long line of victims. Mr. Volach and the Blix team have suffered extraordinary harm from Apple's anticompetitive actions. Blix cannot invest in new software for MacOS, to serve consumers who use MacOS, if they do not receive fair access to the MacOS App Store.

15. Unless consumers have access to Blix's software on all platforms, including the MacOS platform, Blix's software cannot succeed as a cross-platform messaging solution that services *all* of a company's users. Without the ability to reach MacOS users, Blix's software cannot serve enterprise users who prefer MacOS, and its success in the marketplace for cross-platform messaging solutions is at grave risk. Indeed, this underscores the anticompetitive intent and effect behind Apple's actions, which, on information and belief, are not just limited to Blix's BlueMail software. Messaging solutions with cross-platform capabilities (such as BlueMail) are a threat to Apple's dominance.

16. Apple's unlawful conduct is not limited to its misappropriation of Blix's patented ideas, or its unlawful attempts to harm competition by, *inter alia*, excluding Blix's software from the MacOS App Store. Apple's pattern of anticompetitive behavior extends to its treatment of Blix and similarly-situated competitors in Apple's iOS App Store, and extends far beyond cross-platform messaging solutions.

17. Since shortly after the iPhone's inception, Apple recognized that it needs to permit at least the image of choice regarding the apps consumers may use on their smartphones;

otherwise, those users will opt for more open mobile platforms. Apple recognized this by introducing the iOS App Store about a year after releasing the iPhone. But, since it created the App Store, Apple has limited *actual* choice and used its dominance over the iOS App Store to advance Apple's own financial interests at the expense of fair competition. In that process, Blix and a multitude of other competing app developers were unfairly denied a fair opportunity to provide innovative iOS software and obtain substantial market share. Likewise, consumers in the iOS ecosystem were (and continue to be) denied a fair opportunity to discover and utilize innovative software like BlueMail, and instead were (and continue to be) coerced and misled into using Apple's default apps.

18. Apple has foreclosed competition, and harmed the developers who would otherwise compete fairly for consumer loyalty, through a variety of means. One is (similar to the situation with the Mac App Store) its stranglehold on iOS app distribution and its decisions regarding to which apps it permits or denies access to the iOS App Store. Apple refuses to let other iOS app distribution channels operate; all iOS app developers *must* subject themselves to Apple's iOS App Store, and thus, to Apple's anticompetitive requirements and control.

19. For the apps Apple does permit on the iOS App Store, Apple still forecloses fair competition, by manipulating what that App Store shows consumers when a consumer searches for an iOS app. Apple suppresses search results for competing products, promotes Apple's own applications at the expense of fair competition, and makes it difficult for users to find and install quality replacements for Apple's default apps.

20. Furthermore, as discussed above and herein, Apple forecloses competition by raising rivals' costs through a number of means. Those include rules that expose Apple's rivals, but not Apple, to user ratings and negative feedback. Managing user feedback and responding to

reviews and ratings can be costly; Apple imposes those unique costs on its rivals, but exempts Apple's own software from the iOS App Store rating system. Apple likewise raises rivals' costs when it routinely misappropriates its competitors ideas, without permission, by scrutinizing and reverse-engineering features in apps submitted to Apple for distributed through Apple's iOS App Store. Once that misappropriation is complete, Apple frequently either forces those apps off the App Store or renders them undiscoverable or unattractive to interested consumers.

21. Users should have access to the best software, selected through fair competition on the merits. That process will drive innovation, ensure fair pricing, and increase demand for cutting-edge technologies. Apple harms that process by using its ownership of the App Stores to continuously and unfairly tilt the playing field in its favor.

22. This lawsuit seeks to remedy Apple's many wrongs. Apple is not allowed to steal Mr. Volach's ideas, toss Mr. Volach's BlueMail application out of the MacOS App Store, skew search results in Apple's favor and against its competitors in the iOS App Store, or otherwise stack the deck against competition in many and disparate ways. Apple cannot unlawfully leverage its dominance over the MacOS and iOS App Stores to capture additional market share for its own offerings at the expense of competing technologies. Plaintiff asks this Court to protect its patented inventions, ensure its innovative ideas are not used without permission or compensation, and restore competition to the relevant markets alleged herein.

NATURE OF THE ACTION

23. This is an action for patent infringement arising under the Patent Laws of the United States, 35 U.S.C. §§ 1, *et seq*., and for antitrust violations under the Sherman Act, 15 U.S.C. §§ 1 *et seq*.

24. Plaintiff filed this lawsuit to stop Defendant's unlawful infringement of Plaintiff's patented inventions, to halt Defendant's unlawful effort to maintain and extend monopolies by illegally blocking competition, and to obtain damages, an injunction, and other relief.

THE PARTIES

25. Plaintiff Blix Inc. is a Delaware corporation with its principal place of business in 101 Hudson Street, Jersey City, New Jersey. Blix is the successor by merger to BlueMail Inc. BVI and BlueMail LLC, the entities that first developed BlueMail, and is the exclusive owner of all claims, including antitrust claims, arising from the injuries Apple caused to the BlueMail business.

26. Defendant Apple Inc. is a California corporation headquartered in Cupertino, California. Apple operates retail stores throughout the country, including in this District, where it sells iPhone and iPad devices preloaded with iOS 13 software—including software specially configured for the infringing features of the "Sign In With Apple" service.

JURISDICTION AND VENUE

27. Plaintiff's claims for patent infringement arise under the patent laws of the United States of America, 35 U.S.C. §§ 1 *et. seq*., including 35 U.S.C. § 271. Plaintiff's claims for antitrust violations arise under the Sherman Act, 15 U.S.C. §§ 1 *et seq*., including 15 U.S.C. § 2. This Court has exclusive subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337 and 1338(a).

28. Apple is subject to this Court's personal jurisdiction. Apple has infringed the '284 patent in Delaware by, among other things, engaging in infringing conduct within and directed at or from this District. For example, Apple has purposefully and voluntarily placed its infringing products as described herein into the stream of commerce with the expectation that

these infringing products will be used in this District. On information and belief, these infringing products, including devices running iOS 13 such as iPhones and iPads, have been and continue to be used in this District.

29. Apple employs individuals and operates a retail store at 125 Christiana Mall in Newark, Delaware in this District. Upon information and belief, this store sells more infringing iPhones than any other Apple retail location in the country, and sells and/or supports the second-highest volume of infringing products out of any Apple retail location in the country.[1]

30. Consumers and software developers use the infringing "Sign In With Apple" service with Apple devices throughout the District. Apple has provided the "Sign In With Apple" system, including iOS 13 software containing "Sign In With Apple," to software developers in this District. Apple is also selling devices running iOS 13 to consumers in this District, and pushing software updates to users in this District. As discussed herein Apple has specifically instructed software developers, as well as end-users of Apple devices, to use the infringing features of "Sign In With Apple."

31. On information and belief, "Sign In With Apple" is already live on iOS 13 devices being sold in this District, and being offered as a software update to existing iPhone and iPad devices in this District. On information and belief, users in this District are already using the infringing service—for example, to sign in and communicate with applications such as Kayak and Instacart. On information and belief, infringing aspects of "Sign In With Apple" such as the "Hide Your Email" option are available in, and being used in, this District.

[1] *See* Ex. 2, "Apple's (AAPL) Delaware Store Claims Title for Selling Most iPhones," http://abcnews.go.com/Business/apples-delaware-store-claims-title-selling-iphones/story?id=20650009.

32. Apple has repeatedly availed itself of the jurisdiction of this Court by filing complaints for patent infringement in this District (*see, e.g.*, *Apple Inc. v. HTC Corp. et al*, C.A. No. 11-611-GMS; *Apple Inc. v. HTC Corp. et al*, C.A. No. 10-544-GMS; *Apple Inc. v. HTC Corp. et al*, C.A. No. 10-167-GMS; *Apple Inc. v. HTC Corp. et al*, C.A. No. 10-166-GMS; *Apple Inc. v. Atico Int'l USA Inc. et al*, C.A. No. 8-283-GMS).

33. This Court also has personal jurisdiction over Apple because, as alleged herein, it has transacted business in this District; directly or indirectly sold or marketed substantial quantities of its products and services in this District; and engaged in anticompetitive conduct that was directed at, and had a direct, substantial, and reasonably foreseeable and intended effect of causing injury to, the business or property of persons and entities residing in, located in, or doing business in this District. Apple has conducted business in this District, and it has purposefully availed itself of the resources and the benefits of conducting business in this District. These activities, among others, give rise to Blix's antitrust claims.

34. Venue is proper in this Court pursuant to 28 U.S.C. §§ 1391 and 1400 because Apple has a regular and established place of business in this District, is subject to personal jurisdiction in this District, regularly conducts business in this District, and has committed and continues to commit acts of direct and indirect patent infringement in this District. Venue is also proper in this judicial district under 28 U.S.C. § 1391 because a substantial portion of the events or omissions giving rise to Blix's claims occurred in this District.

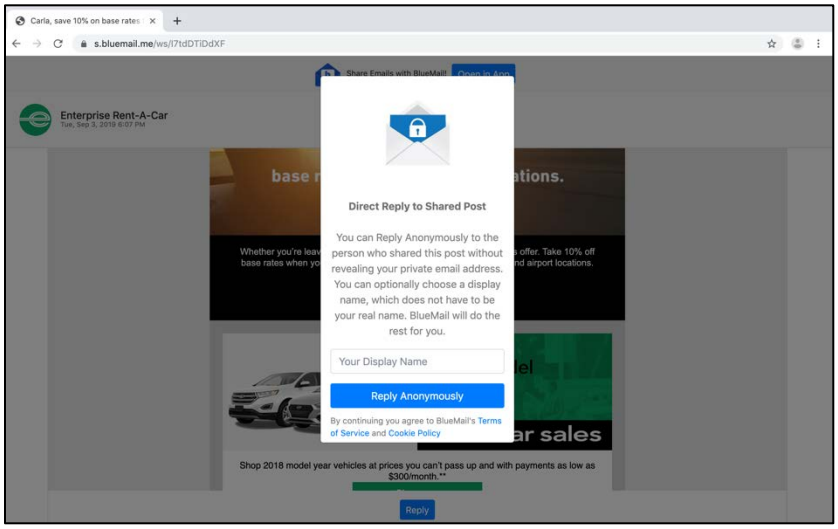
FACTUAL BACKGROUND

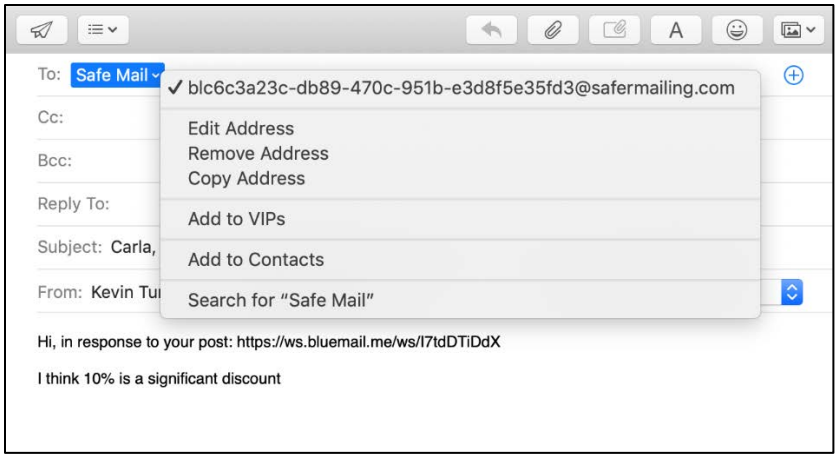
Plaintiff's Cutting-Edge Email Services

35. Plaintiff's BlueMail email service is one of the world's leading email clients. BlueMail has repeatedly won awards for its innovative features and its first-in-class user experience.

36. BlueMail's success extends to multiple platforms. BlueMail was recently ranked #1 on Android Authority's list of "Top Email Apps For Android."

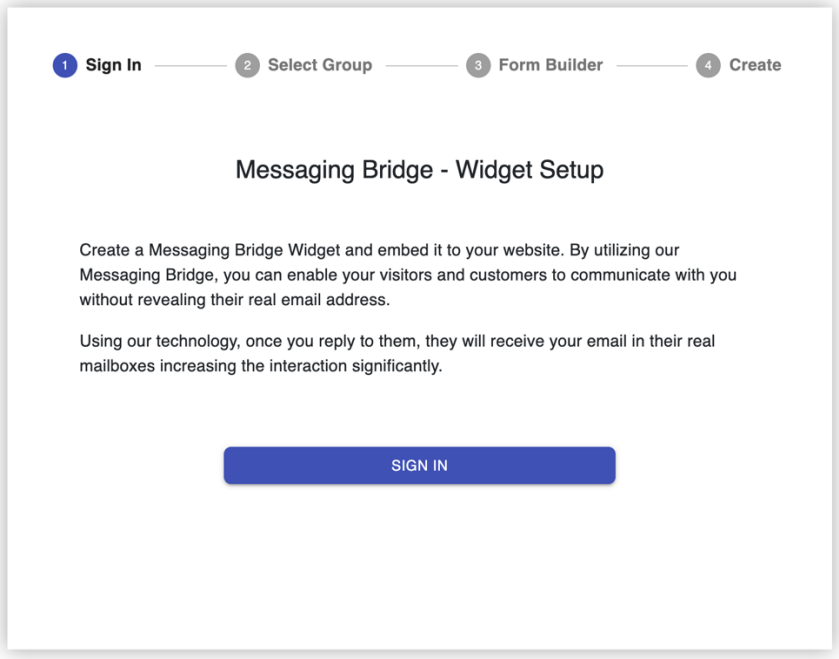
37. BlueMail's success is driven by its innovative features, including its "Share Email" feature. Using this feature, BlueMail users can post an email to social media platforms, such as Twitter, and can then engage in secure private messaging with others. For example, a business could share an email regarding upcoming discounts on social media, and potential customers could engage in direct communication with the company about that upcoming sale using a manageable *public* interaction address BlueMail automatically provides—so that the potential customer's *private* email address is never revealed to the business.





38. Blix is an evolutionary step forward, and builds on BlueMail's innovative messaging features. Blix is a combined email and messaging platform for companies. It allows users of companies to interact with each other via chat service internally, while interacting with the outside world over email.

39. A major capability of Blix is its Messaging Bridge, allowing a Blix customer to engage visitors to their company website through anonymous interactions with the customer's employees, without revealing their real email addresses.



40. The Blix service has been in active development for more than two years, since March 2017. It was launched in September 2019.

41. Blix's business model is based on selling cross-platform messaging services to companies, to meet all of their messaging needs. The employees of these companies typically run a variety of OS platforms, including MacOS. If Blix is unable to serve Mac OS users, many companies may choose not to work with Blix, and may choose offerings from competing companies instead – for example, Apple.

42. Apple's effort to beat Blix to market, using Blix's own patented technology, substantially threatens Blix's ability to obtain market share—and perhaps to continue operations at all.

The Patent-In-Suit

43. On August 29, 2017, the United States Patent and Trademark Office ("the USPTO") duly and legally issued U.S. Patent No. 9,749,284, titled "Systems and Methods of Controlled Reciprocating Communication."

44. Blix is the owner by assignment of the '284 patent.

45. A true and accurate copy of the '284 patent is attached hereto as Ex. 3.

46. The claims of the '284 patent describe an innovative improvement to the operation of communications networks, and specifically, to the ability to manage interactions on communications networks, including a specific architecture to manage interactions employing both private and public interaction addresses. The '284 patent recites a number of implementation details that offer an innovative solution to the problems of privacy and security in modern communications networks. These implementation details include the use of specific private and public interaction addresses in a communications network; records and reverse lists

stored in non-transitory computer storage to associate addresses in a specific manner, to facilitate their management; and specific logic to create, manage, and synchronize address information in a variety of interactions and pre-interactions. This improves the ability of prior art communications systems to facilitate anonymous and easy-to-manage methods of communication.

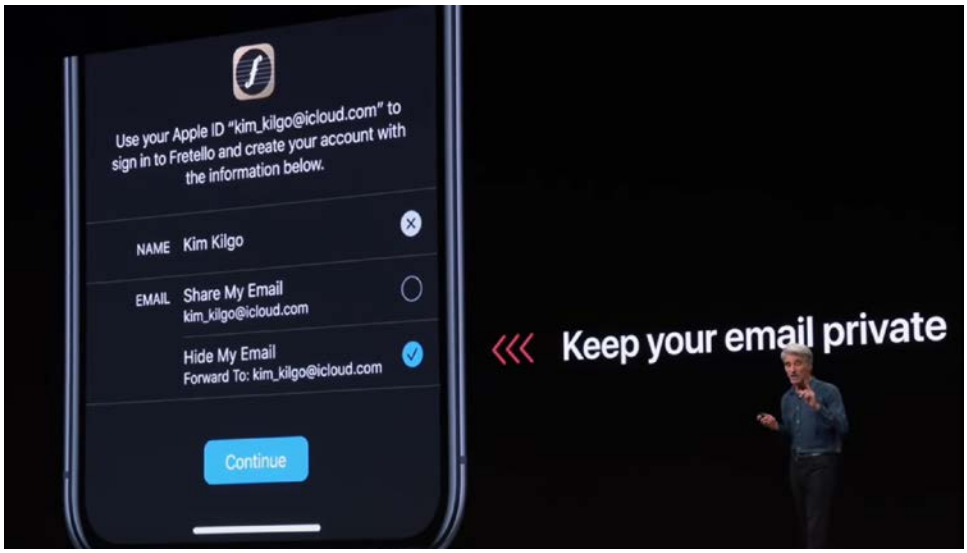
47. In this way, the '284 patent claims do not simply recite, without more, the mere desired result of anonymously communicating across a communications network in an easy-to-manage method. Rather, the claims recite a specific solution for accomplishing that goal.

Apple's Infringement

48. On June 3, 2019, Apple announced its new "Sign In With Apple" service. Apple's Senior Vice President of Software Engineering Craig Federighi unveiled the service, including its use of public interaction addresses to mask private interaction addresses, to extended and thunderous applause.[2] Mr. Federighi explained that Apple, like many software developers, recognized the growing need for a system to manage interaction addresses and protect privacy; "personal information" too often "gets shared" through online communication, something Apple "wanted to solve" though its new "Sign In With Apple" service.

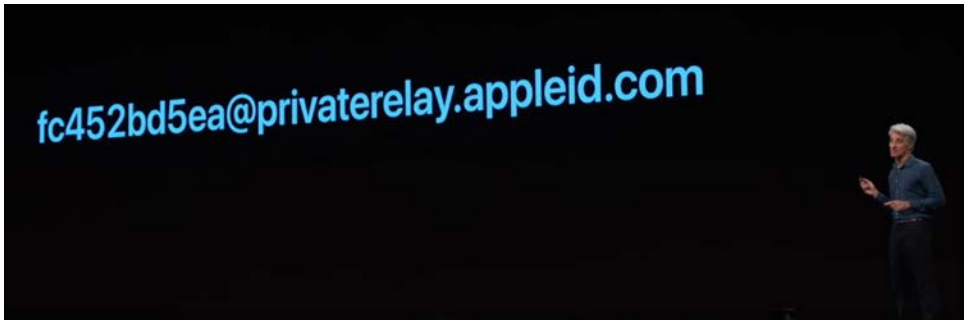
[2] A video of the Keynote presentation from Apple's 2019 Worldwide Developer Conference is available online at https://developer.apple.com/videos/play/wwdc2019/101/. An excerpt from Apple's transcript of that presentation, taken from the same website, is attached. *See* Ex. 4.

49. Mr. Federighi described the service as "the fast, easy way to sign in without all of the tracking." This system used a new application programming interface (API) that would permit users to log in to and communicate with applications in a new and more private manner: "you are authenticated with Face ID on your device, logged in with a new account without revealing any new personal information." Users would be able to log in, but "Keep your email private":



50. As Mr. Federighi explained, the new system worked by assigning public-facing random addresses for the application to interact with the user. These interaction addresses were

intended to be easily manageable, relaying communications from public interaction addresses to private interaction addresses using "a unique random address that forwards to your real address."



51. Apple's head of software further explained that this private relay system would assign multiple interaction addresses to facilitate a user's ability to manage interactions with applications; each user would receive a separate interaction address for interactions with specific developers: "we give each app a unique random address. This means you can disable any one of them at any time when you are tired of hearing from that app. It's really great."

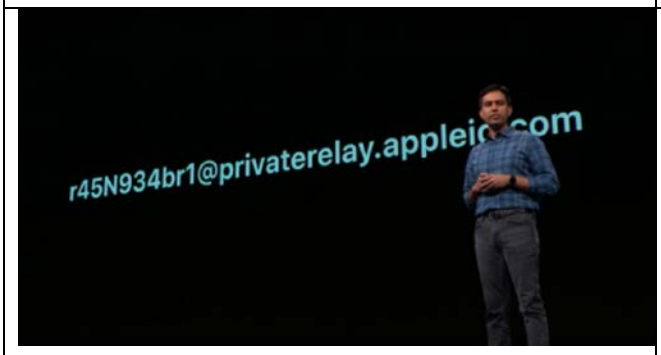
52. Apple's head of software further explained that Apple was offering this system for manageable communications to protect the privacy of users, and to respond to growing demand among users: Giving third parties your electronic addresses information "can be convenient, but it also can come at the cost of your privacy. Your personal information

sometimes gets shared behind the scenes and these log ins can be used to track you. We wanted to solve this and many developers do too." But the solution Apple used was not Apple's to use—it was the same system Mr. Volach had already patented several years earlier.

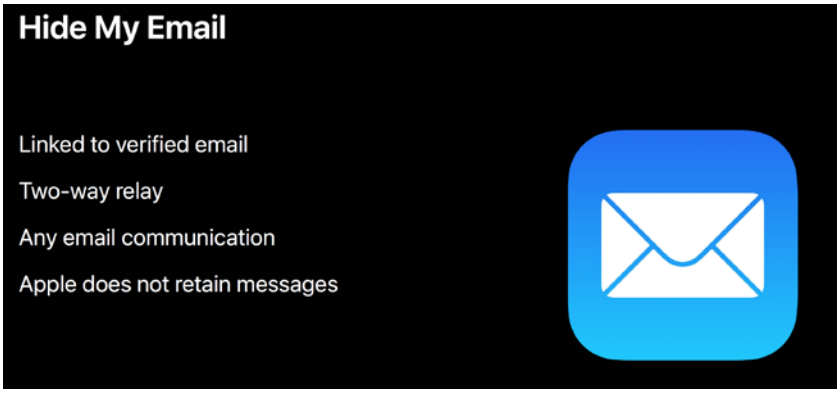
53. In other presentations at Apple's Worldwide Developer Conference in June 2019, Apple continued to encourage software developers to use infringing features of the "Sign In With Apple" service in their software applications. For example, after the keynote address, three Apple engineers gave a separate presentation entitled "Introducing Sign In With Apple."[3] During this hour-long presentation, Apple's engineers gave a large crowd of software developers detailed instructions on how to use infringing "Sign In With Apple" functionality. Those engineers explained that users would often create a host of false, hard-to-manage public interaction addresses to protect their privacy:

[3] A video of this presentation is available online at https://developer.apple.com/videos/play/wwdc2019/706/. An excerpt from Apple's transcript of that presentation, taken from the same website, is attached. *See* Ex. 5.

54. Apple touted its "Private Relay" service as the solution to this problem, noting that the "Sign In With Apple" system would automatically create email addresses shared between the end-user and the application developer. A developer's emails to this address would be automatically forwarded to the user's private addresses, such that the user could receive email while hiding its email address from the application developer:

Randomly-Assigned Address Is Shared	Private Address Stays Hidden
	

55. Apple touted this "Hide My Email" and "Private Relay" system as a significant step forward in protecting user's privacy, while still enabling easy-to-manage electronic communication. Apple encouraged software developers to use the new API that Apple would be releasing for Apple devices (such as iPhones and iPads running iOS 13), claiming that the API offered a solution for users who desire privacy because its "Hide My Email" features would enable a private "Two-way relay" for "Any email communication" between parties:



56. In another presentation entitled "Designing for Privacy," Apple engineers instructed developers to use infringing features of "Sign In With Apple" in their applications in order to more effectively reach customers concerned with privacy: "we think this is your best shot at getting your emails in front of your customers."[4] Apple engineers acknowledged that "People can be hesitant to share their real email address" because of privacy problems created by sharing interaction addresses; "We've all seen email lists stolen or resold and then abused by spammers." Apple employees described Apple's new private relay service and "Sign In With Apple" as the best way to facilitate interaction without sharing private interaction addresses:

> Customers can choose to hide their email address, in which case you'll get an address managed by Apple through which we relay your emails to the customer and vice versa…
>
> For each customer, this managed address is different for each developer, so customers are in control of which developers they want to receive email from, and you're in control of who can send emails to the managed address we provide you, since you can whitelist domains or addresses that we'll accept incoming mail from.

57. This presentation by Apple engineers further explained that the code in Apple's new API for "Sign In With Apple" was specifically configured to enable trusted interactions, allowing a software developer to know they are communicating with the intended user even without knowing the user's private interaction address: "With Sign In With Apple, we can leverage on-device intelligence to provide you with one bit that indicates a user is likely real. And that flag is supported on iOS, and we provide it at account creation."

58. Apple's website offers further instructions to developers and end-users on how to utilize infringing aspects of the "Sign In With Apple' service.

[4] A video of this presentation is available online at https://developer.apple.com/videos/play/wwdc2019/708/. An excerpt from Apple's transcript of that presentation, taken from the same website, is attached. *See* Ex. 6.

59. For example, Apple tells developers that "Sign In With Apple was built from the ground up to give users peace of mind about their privacy," because it offers a secure and private platform for anonymous messaging: "Apple's private email relay lets users receive email even if they prefer to keep their address private."[5] Apple likewise tells end-users to use the infringing features of "Sign In With Apple." For example: "Sign in with Apple is the fast, easy, and more private way to sign into apps and websites using the Apple ID that you already have."[6]

60. Apple further instructs developers to use Apple's "Private Email Relay Service" to meet user's growing demand for a private and secure communication system that protects their privacy. Apple tells third-party software developers that "Some privacy-conscious users will choose to keep their personal email address private and use Apple's private email relay service when setting up an account. To send email messages through the relay service to the users' personal inboxes, you will need to register your outbound email domains."[7] Apple likewise instructs end-users to use the infringing features of Sign In With Apple: "You can use Hide My Email—Apple's private email relay service—to create and share a unique, random email address that forwards to your personal email. That way you can receive useful messages from the app without sharing your personal email address. Only the registered app or site developer can communicate with you using this email, and you can turn it off at any time."[8]

61. Apple's detailed instructions to software developers instruct them to register up to 10 interaction addresses to use for communications with "Sign In With Apple" users. Specifically, Apple tells developers: "In order to send email messages through the relay service

[5] *See* Ex. 7, "Overview: Sign In With Apple," https://developer.apple.com/sign-in-with-apple/.

[6] *See* Ex. 14, "How to use Sign in with Apple," https://support.apple.com/en-us/HT210318.

[7] *See* Ex. 8, "Make Signing In Easy," https://developer.apple.com/sign-in-with-apple/get-started/.

[8] *See* Ex. 14.

to the users' personal inboxes, you will need to register your outbound email domains," that "registered domains must create Sender Policy Framework (SPF) DNS TXT records in order to transit Apple's private mail relay," and that a developer "can register up to 10 domains and communication emails" to communicate with "Sign In With Apple" users through the "Private Email Relay Service."[9] Apple likewise gives detailed instructions to end-users on how to use infringing features for anonymous communication[10] and for interaction address management.[11]

62. Apple's "Sign In With Apple" system clearly infringes Mr. Volach's patented techniques in the '284 patent. Yet Apple never sought permission to use these techniques, never acknowledged to developers that these techniques originated with Mr. Volach, and never offered to pay for using these technologies.

Apple's Pattern of Stealing Ideas and Manipulating Markets

63. Apple's misappropriation of Mr. Volach's ideas is part of a long and well-documented pattern of theft by Apple. Steve Jobs, Apple's co-founder, famously admitted, "We have always been shameless about stealing great ideas."

64. Apple's practice of stealing great ideas extends to ideas Apple finds in the App Store. As the Washington Post recently noted, Apple frequently takes ideas from third-party applications in the App Store, and uses those ideas to build copycat Apple-branded applications: "Apple plays a dual role in the app economy: provider of access to independent apps and giant competitor to them," and "Developers have come to accept that, without warning, Apple can

[9] *See* Ex. 9, "Configure Private Email Relay Service," https://help.apple.com/developer-account/#/devf822fb8fc.

[10] *See* Ex. 15, "Hide My Email for Sign in with Apple," https://support.apple.com/en-us/HT210425#hideemail.

[11] *See* Ex. 16, "Manage the apps you use with Sign in with Apple," https://support.apple.com/en-us/HT210426.

make their work obsolete by announcing a new app or feature that essentially copies their ideas." Ex. 1.

65. Apple's own former director of App Store review Phillip Shoemaker has admitted, "Apple gets a lot of inspiration from apps that are on the App Store." Mr. Shoemaker further confirmed that Apple collected and analyzed App Store data on third-party applications to decide what ideas Apple would include in its own offerings: "Top Apple executives" could "peek at apps under review," and decisions on which new apps to develop were "made at the top rungs of the company." Mr. Shoemaker would then receive "regular emails from angry app developers, irked that the company had rejected their app or, in some cases, killed their app off by copying them." Ex. 1.

66. This pattern of stealing ideas from the App Store often kills off third-party app developers in the process. As the Washington Post observed: "Apple's past incorporation of functionality included in other third-party apps has often led to their demise." Ex. 1.

67. Apple engages in this pattern of stealing ideas from third-party developers in order to maintain its dominance in the marketplace. Stealing ideas is even more critical to Apple now as sales of the iPhone, its most lucrative product, have slowed. To prove its usefulness to consumers, Apple is offering them more and more services – including innovative services copied from third-party offerings in the App Store.

68. On information and belief, Apple's rejection of BlueMail is part of this same pattern: steal great ideas from the App Store, and then discard what remains of the stolen application. This conduct not only violates Blix's intellectual property rights, but, as discussed, also forms a core part of Apple's wide-ranging and extensive anticompetitive conduct.

Apple's Anticompetitive Conduct: Introduction

69. For years, Apple has abused its dominance over MacOS and iOS apps. This is particularly troubling because Apple realized long ago that consumers need at least the illusion of an option to choose the apps and programs they regularly use on their laptops, smartphones, and other computing devices. Had Apple simply provided users its own default apps/programs, and denied access to any other programs (giving consumers zero options to choose), it would have been at a serious competitive disadvantage, because there is no such thing as a one-size-fits-all computer. Furthermore, consumers have over the years developed a strong preference for choice. Thus, although Apple prefers to utilize a "closed garden" approach to its computing platforms, it still must provide at least the suggestion of choice

70. The problems outlined in this complaint, however, show that Apple has, at nearly every step, stacked the deck against competitors that offer quality alternatives to Apple's default apps. As most relevant to Blix, this includes preventing true competition for mail apps on the MacOS and iOS platforms, but it is not just limited to mail apps. In fact, Apple's anticompetitive conduct has involved multiple categories of apps for both platforms, and its anticompetitive scheme includes a number of different, complementary actions, detailed further below. In short, Apple has crippled true competition for its default apps through a "thousand different cuts." This is illegal and must be stopped.

Apple's Complete Dominance and Monopoly Power Over iOS Apps

71. Apple introduced the App Store in July 2008, roughly one year after it introduced the iPhone in June 2007. On information and belief Apple did so because it needed to provide its new iPhone users with choices over the apps they installed and used on the phone; otherwise, they were uninterested in using the smartphone for all its possible uses and would instead seek

out other platforms, including different types of devices, for their different mobile computing needs. On information and belief, Apple realized this fact based on its experience with apps and programs for mobile laptops. Although Apple had long created its own apps for its Mac line of laptops, it also permitted competitors to create programs for those laptops, because it needed to in order to compete with PCs.

72. As Apple's public advertising campaigns demonstrate, Apple has for years used the availability of third-party applications to fuel the demand for the iPhone and for its iOS platform. As one example, Apple grew its iOS ecosystem during the early days of the iPhone by heavily advertising third-party applications and stating, "there's an app for that."

73. Apple has been highly successful in using third-party applications to drive demand for its iOS products, including the iPhone. In the U.S. alone, consumers own nearly 200 million iPhones, and tens of millions of other iOS devices, including iPads. All of those devices run iOS applications.

74. A device running Apple's iOS operating system can only run applications designed for iOS. Applications must be designed to run on a specific operating system, such as iOS, Android, Windows, or MacOS. Once a user selects iOS as their operating system by

purchasing an Apple device, that user can only run applications designed for the iOS operating system on their device.

75. Users who want applications on their iOS devices must download those applications from Apple's iOS App Store; this is a requirement Apple imposes as both a contractual and technical requirement on iPhone users. Those users thus have no alternatives to the iOS App Store for finding and downloading applications on their iOS devices.

76. High switching costs prevent users from switching from one operating system to another operating system after they initially purchase a mobile device. These switching costs increase over time for a variety of reasons, including (among other things) familiarity with the operating system, familiarity with apps on that operating system, hardware purchased to support the devices utilizing that operating system (*e.g.*, power cords, wireless mouse/keyboards, wireless headphones, other device-specific peripherals). Moreover, switching costs for mobile devices have increased dramatically in recent years with the advent of cloud computing, which, *inter alia*, allows users to store their files on the "cloud" (*i.e.*, not directly on their device). Apple's iCloud system and its iOS integration makes users become more and more entrenched on the iOS platform, because they wish to have continued access to their personal files stored in Apple's "cloud."

77. A software developer who wants to reach users of iOS devices must submit her applications to Apple for review and approval to be listed on the iOS App Store. Apple designs iOS so that there is no authorized manner in which users can install iOS applications other than by downloading them in the iOS App Store. Software developers have no alternatives to the iOS App Store for distributing their applications to iOS users.

78. High development costs that are specific to a particular operating system prevent software companies from easily switching development efforts from one operating system to another. Android apps are written in a different programming language than iOS apps. Code written in languages compatible with iOS, and designed to utilize frameworks offered by the iOS operating system, cannot easily be revised to operate in Android. Software developers who specialize in writing code for iOS applications cannot easily be redeployed to write code for Android applications; while companies often develop apps for multiple operating systems, the employees leading those efforts are typically specialized by operating system.

79. Apple does not allow other third-party services to distribute iOS applications. Apple has designed the iOS ecosystem in such a way that no channel of distribution is available for iOS applications other than the iOS App Store. In this way, Apple is significantly different than other companies. For example, in the Android operating system, Android users can download Android applications from multiple application marketplaces – including Google's Play Store, Amazon's Appstore, and Samsung's Galaxy Store. Similarly, Android software developers can distribute their applications through multiple different competing application marketplaces, including Google's Play Store, Amazon's Appstore, or Samsung's Galaxy Store. Apple is different. Apple does not allow users to download iOS apps from competing app stores, and as a result, essentially faces no competition from a competing iOS app store.

80. Apple'secosystem design grants Apple monopoly power over the distribution of all iOS applications sold in the U.S. Apple acquired this monopoly power by making itself the sole and exclusive option to distribute iOS applications to its millions of users, and by dictating the terms under which app developers may offer their apps to iOS users. Apple had and has no justifiable reason for requiring the competitive restraint (due to agreements imposed on

consumers and app developers) that there be no alternatives for iOS application distribution. As the Android ecosystem demonstrates, competition can and does work, including for the distribution of mobile applications.

81. The presence of competition for Android app distribution channels within the Android ecosystem does not place any check on Apple's power within the iOS ecosystem. Android applications cannot run on iOS devices. Thus, iOS users are locked into Apple's iOS App Store as their only source of iOS applications, and cannot enjoy the benefits of competition in or from the Android ecosystem's more open design.

82. For these reasons, Apple is a monopolist and enjoys monopoly power in the U.S. market for iOS applications. Indeed, Apple admits its power over iOS applications is absolute, as it shuts out all alternative channels for iOS app distribution – ostensibly to "protect" customers from malware and other malicious applications. This is a pretextual claim: Google's Play Store, Amazon's Appstore, and Samsung's Galaxy Store each provide similar benefits and facilitate the distribution of trustworthy applications, but (a) compete with each other, and (b) therefore do not enjoy the same type of control over pricing and simple app availability.

83. Apple's refusal to permit alternative iOS app distribution channels leaves developers with fewer choices (in fact, no other choices) to distribute their iOS applications and reach millions of iOS users. And consumers have fewer alternatives (in fact, no alternatives) to discover and download innovative third-party software for their iOS devices. This provides Apple enormous power over app developers that compete directly with its default apps, and it allows Apple to stringently control consumer choice, much to their detriment.

84. Apple's refusal to permit competition reduces incentives to develop iOS applications, reducing output in the market for iOS applications. Software developers who do

not want to agree to Apple's terms and conditions for the iOS App Store have no alternative but to avoid iOS app development altogether. And without competition in the market for iOS app distribution, Apple has no incentive to offer more attractive and competitive terms to developers. Consumers also suffer from Apple's refusal to permit competing iOS app marketplaces, including because fewer iOS app developers means less innovation and fewer software alternatives to select from in the iOS ecosystem. Consumers would benefit from competition between multiple iOS app marketplaces, as competition would drive the development of additional high-quality applications, give consumers additional choices among applications, and give iOS users additional avenues to discovery and install applications.

85. In order to reach iOS users, Blix has been forced to submit its software to Apple for approval, and to distribute its applications to users via the iOS App Store.

86. Because Blix must rely on the iOS App Store to reach consumers, Blix is dependent on Apple offering fair access to consumers in the iOS App Store that Apple controls.

87. As described herein, Apple has not given Blix fair access to consumers, and has instead implemented a variety of barriers to make it difficult for consumers to locate Blix and other innovative third-party software – instead pushing consumers to Apple's own competing software offerings.

Apple's iOS Monopolization: The iOS Email Client Relevant Market

88. An email client is a software application used to send and receive electronic mail. Email clients are local software packages that offer a collection of features designed to facilitate sending, receiving, composing, and organizing email. These local software programs differ from command-line interfaces or from web-based interfaces, which offer a more limited set of features and typically cannot operate locally when a device is not online.

89. Mail clients are software applications designed to run on a specific operating system, such as iOS or Android. Email clients designed to run on one operating system (such as Android) are not substitutes for email clients designed to run on another operating system (such as iOS), since a software package designed to execute on one operating system will not execute on another operating system.

90. Mail clients have a unique purpose vis-à-vis other types of apps: to provide users with the ability to draft, send, and receive emails. Although other types of messaging apps allow users to send and receive messages to each other, those types of messages (*e.g.*, text messages, social media messages, etc.) serve different purposes and are used in different ways by consumers. A consumer will almost always have a mail client app on their smartphone and use that app in parallel to text messaging, social media messaging, and instant messaging. In other words, although messaging solutions have overlapping uses, mail clients are not considered reasonably interchangeable with other types of messaging solutions and are considered a "must have" app for messaging *in addition to* those other types of messaging apps.

91. The geographic scope of the iOS Email Client Market is national.

92. The existence of email clients for operating systems other than iOS is irrelevant to the analysis of the relevant market at issue; software developed for other operating systems is not compatible with iOS devices, and therefore those applications are not reasonably interchangeable substitutes for iOS email clients.

93. Apple pre-installs its own email client, Apple Mail, on all iOS devices. By pre-installing Apple Mail on all iOS devices, Apple has long enjoyed a dominant position in the iOS Email Client Market. Apple's "Apple Mail" application is preinstalled as the default email client for all 200 million iOS users.

94. Apple's decision to offer an email client on iOS was a cornerstone in its overall market strategy. As Apple emphasized when it announced the iPhone on January 9th, 2007, "Apple today introduced iPhone, combining three products—a revolutionary mobile phone, a widescreen iPod with touch controls, and *a breakthrough Internet communications device with desktop-class email*, web browsing, searching and maps—into one small and lightweight handheld device."[12]

95. The importance of software offerings in Apple's iPhone and iOS strategy has grown over time. In 2007, the iPhone had 17 pre-installed apps. Today, there are 38. And since the App Store launched in 2008, Apple has never let consumers set a third-party app as a default option for certain functions—unlike on Android or Windows, where third-party defaults are permitted. For example, Google allows Android users to pick Firefox as their go-to browser relatively easily. Apple does not do this. As Bloomberg noted, based on discussions with antitrust lawyers, "This sounds like Microsoft in the 90s. Back then, the U.S. sued Microsoft Corp. for trying to shut out other web browsers by bundling Internet Explorer with its Windows operating system and making it hard to install replacements."[13]

96. Apple's dominance in the iOS Email Client Market is threatened by competition from innovative entrants, especially BlueMail, that provide a more appealing user experience through a cutting-edge design and a more attractive blend of features to users—including innovative messaging features not available through Apple Mail. BlueMail's anonymous email features compete directly with Apple's aspirations in this area.

---

[12] *See* Ex. 17, https://www.apple.com/newsroom/2007/01/09Apple-Reinvents-the-Phone-with-iPhone/.

[13] *See* Ex. 18, "Apple's Default iPhone Apps Give It Growing Edge Over App Store Rivals," https://www.bloomberg.com/news/articles/2019-10-02/iphone-ios-users-can-t-change-default-apps-safari-mail-music.

97. The patented features in the '284 patent, employed by BlueMail, are highly attractive to end-users. Apple admitted during its 2019 Worldwide Developers Conference that these anonymous communication features solved a pressing problem Apple and many other software developers wanted to solve, to address end-user concerns and meet market demands: electronic communication "can be convenient, but it also can come at the cost of your privacy. Your personal information sometimes gets shared behind the scenes and these log ins can be used to track you. We wanted to solve this and many developers do too." Ex. 4.

Apple's Exploitation of its Dominance Over iOS App Distribution: Suppressing Consumers' Ability to Locate or Even Obtain Quality App Competitors

98. The iOS App Store's "Search" feature is the primary interface for users to search for applications by keyword in the iOS App Store. In July 2019, according to the WSJ "Rankings from search results in Apple's store can make or break an app. The company [Apple] says searches lead to 65% of all app downloads."[14]

99. Search ranking is critical for app developers to reach potential users. When a user searches for an application, they are very likely to select one of the first applications they encounter in their search results. As the New York Times recently reported, "[t]op spots in App Store search results are some of the most fought over real estate in the online economy." Accordingly, "[t]o get their apps discovered, companies try to push them up the ranks in the App Store's search results. There is an industry of consultants who charge for their expertise on setting the right title, description and other details to please the App Store algorithm."

100. Apple designs and controls the Search interface in the iOS App Store.

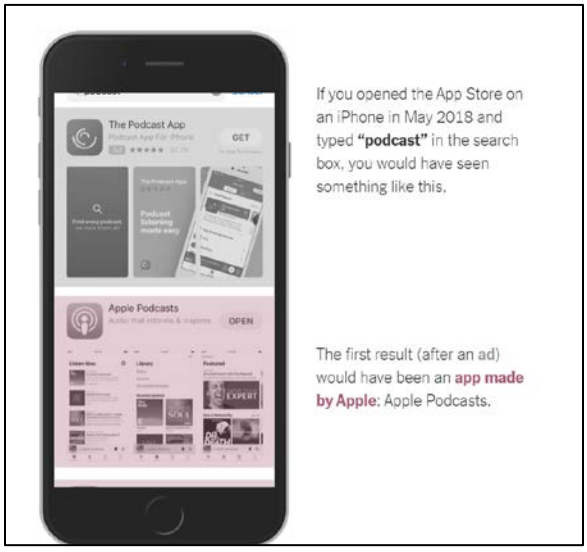
[14] *See* Ex. 19, "Apple Dominates App Store Search Results, Thwarting Competitors," https://www.wsj.com/articles/apple-dominates-app-store-search-results-thwarting-competitors-11563897221.

101. For years, Apple manipulated the Search feature in its iOS App Store to push consumers away from third-party software and towards Apple's own software offerings. Additionally, Apple intentionally took steps to "lock in" competition from a limited number of players in key application categories, including the mail application category, to impose additional barriers to entry for new and innovative software in those categories – ensuring that Apple would face substantial competition from only a known group of existing entrants.

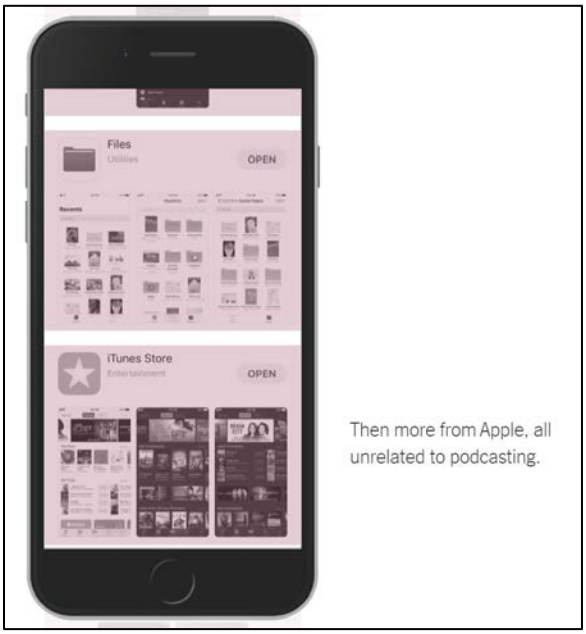
102. As the New York Times noted recently, "suspicions that the company has been tipping the scales in its own favor are at the heart of antitrust complaints in the United States, Europe and Russia."

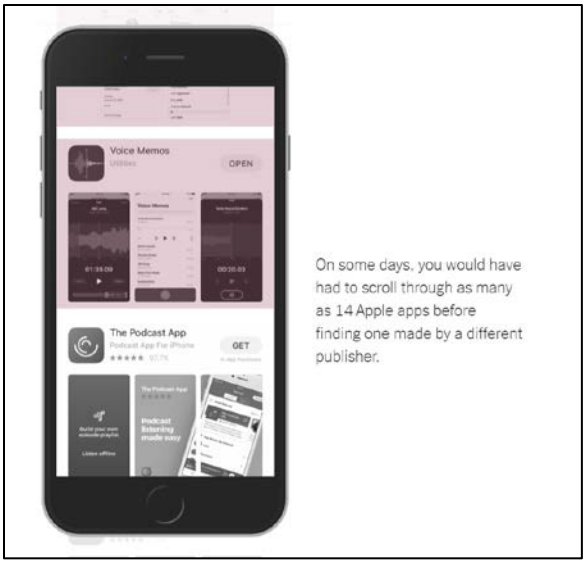
103. Apple has used its control of the iOS App Store to artificially inflate Apple's search ranking for a variety of keywords and in a variety of categories. Apple does this to award itself the coveted top spots when a user searches for apps.

104. As the New York Times reported, "Apple's apps have ranked first recently for at least 700 search terms in the store," and "[s]ome searches produced as many as 14 Apple apps before showing results from rivals":




273° W
Find My Friends
Social Networking
OPEN
Tips
Utilities
OPEN
The next result would have been Apple's Compass app.
Then its Find My Friends app.


Files
Utilities
OPEN
iTunes Store
Entertainment
OPEN
Then more from Apple, all unrelated to podcasting.

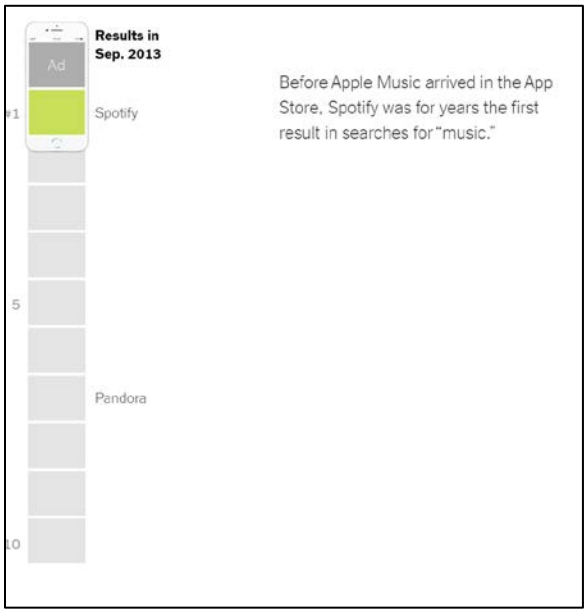


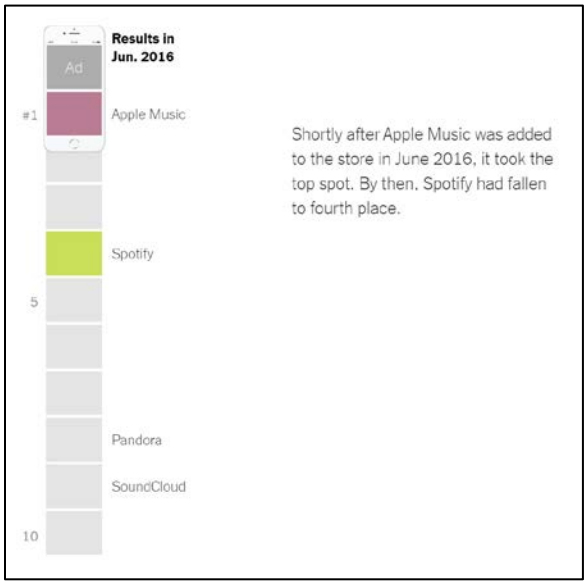
105. When presented with the New York Times' analysis of the iOS App Store, and confronted with evidence of Apple's efforts to artificially inflate the search rankings of Apple software, "two senior Apple executives acknowledged [to the New York Times] that, for more than a year, the top results of many common searches in the iPhone App Store were packed with the company's own apps." These executives further admitted that this "was the case even when the Apple apps were less relevant and less popular than ones from its competitors."

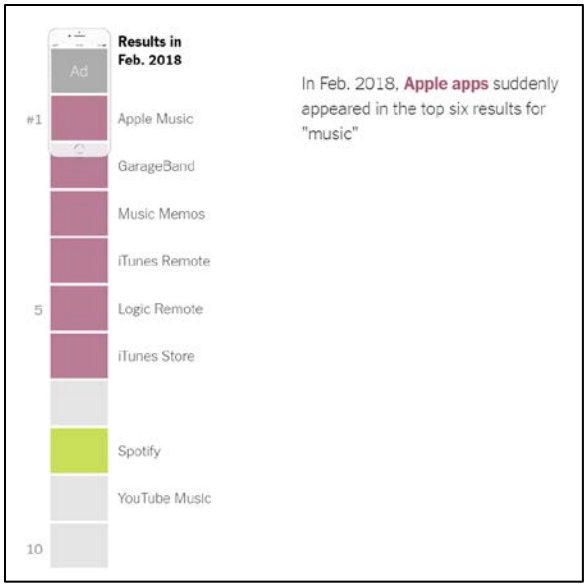
106. Caught red-handed, Apple admitted that "the company had since adjusted the algorithm so that fewer of its own apps appeared at the top of search results." But Apple's pattern of manipulating search results in order to promote its own apps at the expense of competitors appears to have persisted for years – apparently beginning in or around June 2016, when Apple began offering its own apps in the iOS App Store.

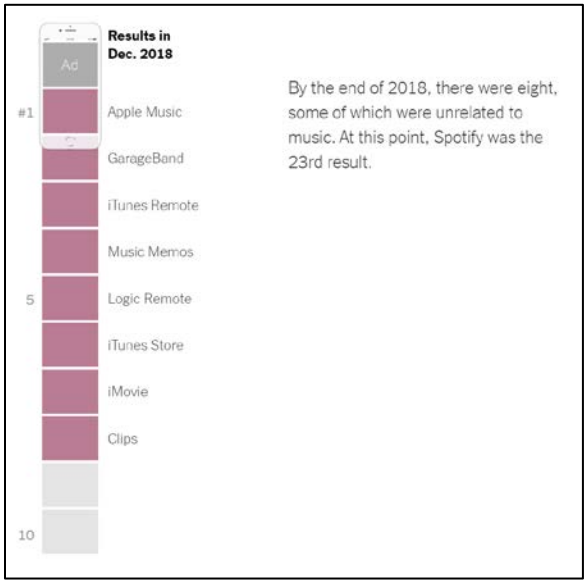
107. According to a New York Times analysis, when Apple first introduced its applications to its iOS App Store, Apple *immediately* took the top search result for many popular search terms, and "Apple apps held on [to that search ranking] for years while top rivals remained stuck below, sometimes hundreds of slots down the list."

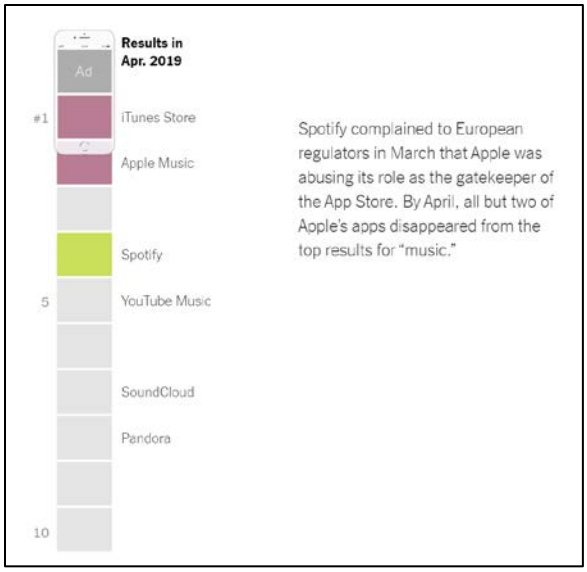
108. This was vividly illustrated by the New York Times, which chronicled Apple's quick rise to the top of – and then occupation of nearly the entirety of – the top 10 search rankings for keywords such as "music."






Results in Feb. 2018
Ad
#1
Apple Music
GarageBand
Music Memos
iTunes Remote
5
Logic Remote
iTunes Store
Spotify
YouTube Music
10
In Feb. 2018, Apple apps suddenly appeared in the top six results for "music"


Results in Dec. 2018
Ad
#1
Apple Music
GarageBand
iTunes Remote
Music Memos
5
Logic Remote
iTunes Store
iMovie
Clips
10
By the end of 2018, there were eight, some of which were unrelated to music. At this point, Spotify was the 23rd result.



109. The New York Times' Sept. 2019 report also explained that experts in the search field agree Apple has intentionally manipulated search rankings to promote its own applications, at the expense of competitors, finding it "hard to believe that organically there are certain Apple apps that rank better than higher-reviewed, more downloaded competitors."

110. The New York Times offered other examples in its Sept. 2019 report to illustrate Apple's manipulation of search rankings and its promotion of Apple's own applications, at the expense of Apple's rivals. For example, "[o]n March 25, the company unveiled an Apple-branded credit card that can be used via the Apple Wallet app. The next day, Apple Wallet was the No. 1 result in searches for 'money,' 'credit' and 'debit.' The app had not ranked for those search terms before then."

111. On information and belief, Apple manipulated App Store search results, including the ranking of applications in response to searches for popular keywords, to suppress the popularity of results from competitors – including Blix's innovative BlueMail application. Apple's manipulation of search rankings inhibited consumers' ability to discover quality competitors to its default mail client app (including BlueMail), harmed competitors' (including

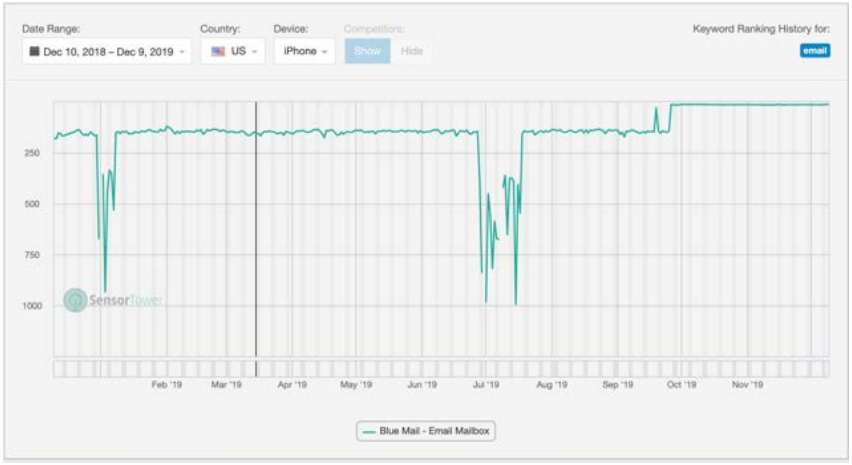
BlueMail's) ability to reach consumers, and injured those competitors' (including BlueMail's) ability to compete with Apple's own Apple Mail offering.

112. On Android, where BlueMail was given fair access to consumers, BlueMail reached millions of consumers and received approximately 525,000 reviews (almost all of them positive). But on iOS, where BlueMail was suppressed in Apple's search rankings, BlueMail reached far fewer consumers and was reviewed only 4,200 times.

September 26, 2019: Apple's App Store Radically Changes Rankings

113. Shortly after the New York Times's September 9 story on Apple's manipulation of App Store search results, Apple's search rankings changed dramatically. On information and belief, Apple changed its search algorithms in an apparent attempt to remove the techniques for manipulation and suppression that it had previously employed and that were now under scrutiny in the wake of the New York Times' extensive report.

114. Days after the New York Times story published, BlueMail shot from #143 to #13 on simple keywords such as "email" in the iOS App Store – despite *no change* in the BlueMail iOS application itself.



115. BlueMail was not the only Apple Mail competitor to experience this sudden change in search ranking suppression. For example, YandexMail (another competing mail client)

jumped in the search rankings for "email" from approximately #160 to #32 on September 26, 2019.

116. This was not just limited to iOS mail clients. On information and belief, given the widespread nature of Apple's reported search result-stacking, this same practice harmed competition for multiple different categories of apps that compete with Apple's default apps, and multiple different types of Apple app competitors enjoyed a sudden, unexplained rise in search rankings following the New York Times expose.

117. In addition to suppressing search results showing the highest-quality alternatives to its default apps, Apple has also taken a number of other affirmative steps to abuse its monopoly over iOS applications and protect Apple's own applications from fair competition.

118. *First*, as noted above, Apple has designed the iOS App Store so that Apple's own applications are the top-ranked search result in response to a number of application keywords, including "mail" and "email." This makes it harder for consumers to discover competing applications such as BlueMail.

119. On information and belief, users rarely if ever select search results outside the top 20 to 25 results for a given query. On information and belief, users frequently only review the very top results for a typical keyword query.

120. By designing Apple's search algorithms such that competitors (but not Apple) fall outside the top-ranked results for a given search, Apple effectively forecloses competition. If consumers will only review the top search results, Apple can create the illusion of competition – but in fact, foreclose competition – by ensuring that Apple's applications occupy the top positions in a search ranking.

121. On information and belief, Apple specifically designed its iOS App Store search algorithms to ensure that Apple's applications – not competitor applications – would enjoy the top-ranked position for keyword searches such as "mail" and "email."

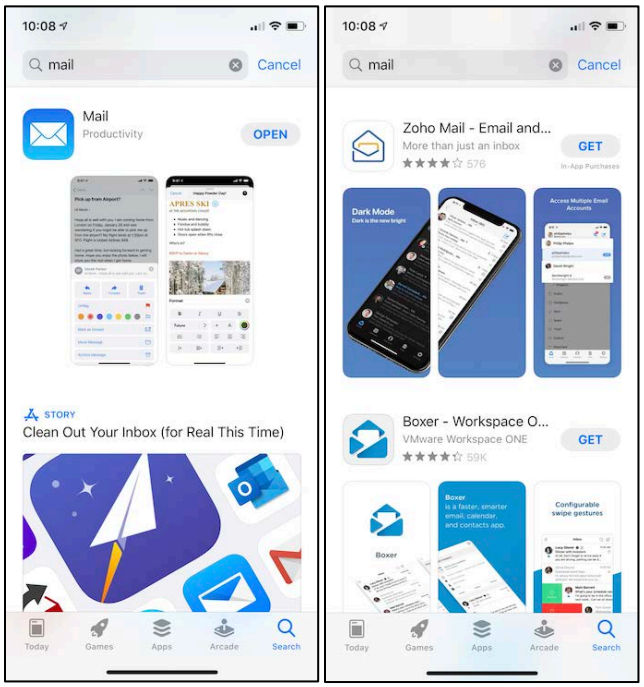
122. *Second*, Apple exempts its own applications – *but not its competitors' applications* – from user-submitted rankings and feedback. This exemption prevents users from easily determining whether Apple's default apps stack up, quality-wise, to its competitors' apps, and further shields Apple from the same type of feedback that it imposes on competitor app developers in order to appear in the iOS App Store.

123. For example, third-party applications in the iOS App Store can be rated by users (*e.g.*, five stars, four stars, three stars). Third-party applications can also be reviewed by consumers. This exposes third-party application developers to the risk of negative user feedback. Low ratings and negative reviews can harm an app developer's standing with consumers, and ostensibly should lead to lower placement in search results on the App Store.

124. Apple's default applications, such as its Mail application or Books application, *cannot* be rated by users – insulating Apple software from the risk of negative reviews or low ratings. Specifically, Apple designed the iOS App Store in such a way that users are not allowed to submit a rating (like a two-star or three-star review) for certain Apple applications. Thus, Apple immunizes itself from a form of competition its competitors must all face – effectively

making Apple the only software developer whose apps are listed (usually as the first result) without any negative feedback or comments.

125. In the picture below, Apple Mail is shown without any ratings and reviews while Zoho Mail and Boxer show reviews and ratings.

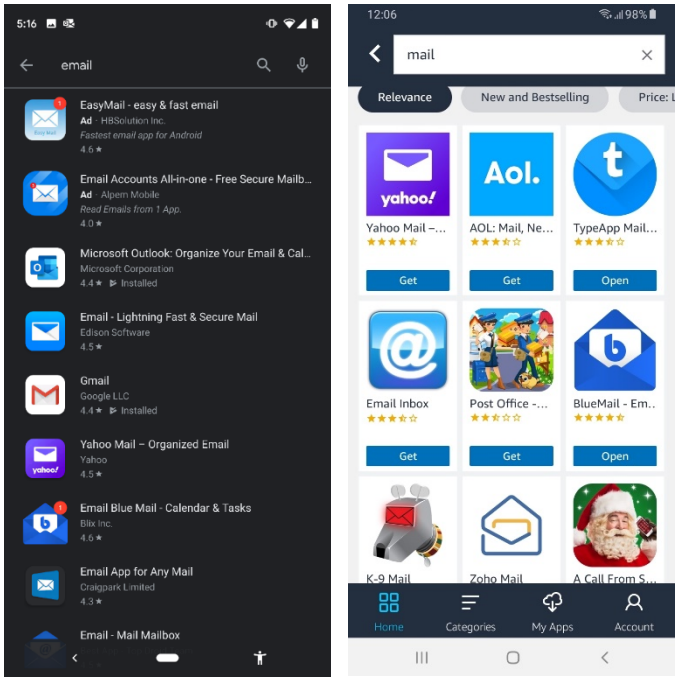


126. Apple chose to eliminate rankings for its own applications in order to protect those applications' placement in the App Store. According to the WSJ, Apple has intentionally made decisions about App Store design that benefit Apple's own applications over competitors. For example, an "Apple app, Podcasts, previously averaged a 1.7-star rating before reviews [for the application] were eliminated, according to Sensor Tower." Ex. 19. Apple avoided taking steps that would improve application quality in the App Store at the expense of its own offerings. For example, "Phillip Shoemaker, who led the App Store review process until 2016, said Apple executives were aware of Podcasts' poor ratings. Around 2015, his team proposed to senior executives that it purge all apps rated lower than two stars to ensure overall quality. 'That would kill our Podcasts app,' an Apple executive said, according to Mr. Shoemaker." *Id.*

127. *Third*, on information and belief, Apple intentionally designed the iOS App Store in a manner that increases user search costs and discourages users from evaluating a high number of applications in response to any particular query.

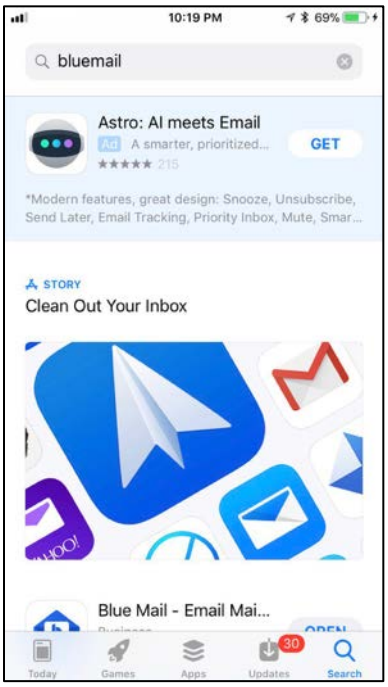
128. Apple's layout for the iOS App Store's "Search" feature forces a user to scroll significantly in order to reach many – and sometimes any – third-party applications. Unlike other application marketplaces, Apple takes up significant room in the earch interface for paid advertising and Apple-selected "Stories" featuring only the applications Apple chooses to make discoverable by users, to the point where a user's requested application may not be visible (or may be barely visible).

129. As shown below, when a user searches the Google Play Store (on the left) or the Amazon Appstore (on the right), users are immediately offered a variety of applications to choose from. This presentation lowers users' search costs and immediately presents users with a variety of options.



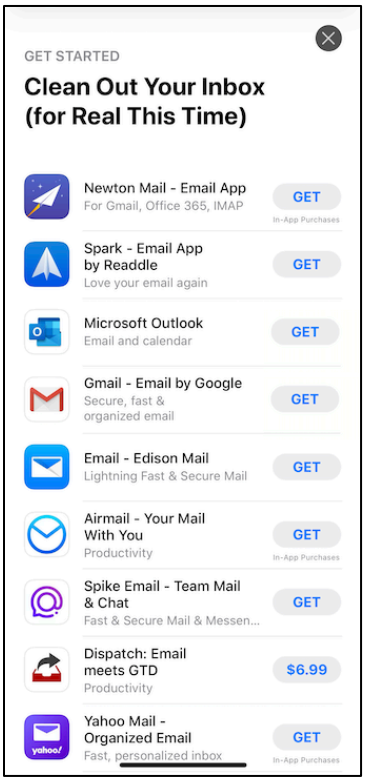
130. Apple, in contrast, designed the iOS App Store user interface to offer users far fewer choices, and to force users to take affirmative action before they can view multiple options.

131. As one example, in response to a direct search for "BlueMail", Apple's iOS App Store has at times been designed to first direct users to a large-sized paid advertisement occupying roughly 30% of the screen. Apple would then direct users to an Apple-selected "Stories" box (an Apple-selected lists of applications) that occupies nearly 50% of the screen. The BlueMail application was barely visible, occupying less than 5% of the screen, as shown below:



132. While the iOS App Store search interface has changed over time, and continues to change, at times relevant to this complaint Apple has used other designs in its "Search" interface to ensure oversized portions of the user interface lead users away from competitors' apps and towards Apple-curated lists or Apple-selected advertisements.

133. Moreover, Apple's "Stories" for categories such as email act as a further barrier to entry and innovation. The iOS App Store interface is designed to draw users to the "Story" before they might encounter a list of other applications. In that "Story," Apple offers only a limited number of email applications that Apple selects – a list that has remained essentially static for nearly 2 years – presenting a significant barrier to entry by new email applications.



134. Fourth, as described above, Apple routinely takes steps to foreclose competition from competitors' iOS applications. This includes raising rivals' costs by misappropriating smaller competitors' innovations and intellectual property, incorporating that stolen functionality in its own apps, and then either jettisoning the competitor apps from the iOS App Store or otherwise rendering those competing apps non-entities in consumers' eyes, whether due to pushing them down in the App Store search rankings (making them effectively invisible),

hampering their functionality on iOS, or otherwise destroying their ability to compete with Apple's default apps.

Apple's Dominance and Monopoly Power Over MacOS Applications

135. Apple's anticompetitive conduct is not limited to iOS apps. Instead, Apple's conduct is far broader and also encompasses mail clients (among others) for MacOS.

136. High development costs, including costs that are specific to a particular operating system, prevent software companies from easily switching development efforts from one operating system to another. Windows apps are written in a different programming language than MacOS apps. Code written in languages compatible with MacOS, and designed to utilize frameworks offered by the MacOS operating system, cannot easily be revised to operate in Windows (or even mobile operating systems). Software developers who specialize in writing code for MacOS applications cannot easily be redeployed to write code for other operating system applications. Although companies often develop apps for multiple operating systems, the employees leading those efforts are typically specialized by operating system.

137. Apple has been highly successful in using third-party applications to drive demand for its Mac line of computers. Software applications for one operating system are not interchangeable (let alone reasonably so) with applications for a different operating system, because applications for one will not work on the other. Windows applications do not work on MacOS, and vice versa. (The same goes for applications written for other operating systems, such as Linux.) Once a user selects an operating system (*e.g.*, by selecting a Windows computer, a MacOS computer, or some other computer), a market exists for software applications that will run on that operating system. The operating system on one's computer therefore defines the market for applications in which that consumer looks for options.

138. After noting the success of its iOS App Store, Apple opened its MacOS App Store in January 2011. Similar to the iOS App Store discussed above, the MacOS App Store is an online marketplace for software programs designed to run on the MacOS operating system.[15] Apple owns 100% of the MacOS App Store. It staffs the MacOS App Store with Apple employees or agents, and it controls all of the MacOS App Store's sales, revenue collections, business operations, and application approval decisions. Apple encourages all MacOS users to use the App Store as their exclusive source of software applications, pretextually claiming it offers unique security benefits. In reality, the purported security benefits of the App Store do not exist; indeed, the most popular paid utility on the Mac App Store, Adware Doctor, was eventually removed from the App Store as malware.

139. Similar to the iOS App Store, Apple maintains 100% control over which applications it will and will not accept into the MacOS App Store. This gives Apple complete control over third-party software developer's access to the MacOS App Store as a distribution channel. Also similar to the iOS App Store, Apple imposes certain monetary requirements on MacOS app developers that allow it to control price and output for MacOS applications.

140. Apple's design of the MacOS operating system makes the MacOS App Store its own market – one separate and apart from other potential distribution channels for MacOS software. As explained herein, Apple encourages users to only run software applications if those applications are obtained from the MacOS App Store. A large population of consumers (including all consumers who heed Apple's instructions on security) will not engage with any

[15] References to "MacOS" herein refer to Apple's operating system for desktop and laptop computers, also referred to at times by Apple in marketing materials as "Mac OS," "Mac OS X," or "OS X." References to the "Mac OS App Store" refer to Apple's "App Store" marketplace for MacOS software applications, first released by Apple in January 2011.

other distribution channel. Because of Apple's software design choices, the MacOS App Store is not simply a marketplace – it is a separate and distinct distribution channel for MacOS apps that can neither be replicated nor, given the ways in which software are most often obtained for Mac computers, be supplanted. Moreover, the MacOS App Store is the way in which the vast majority of Mac users today obtain their software applications.

141. Today, there are no reasonable substitutes for the MacOS App Store, either for consumers seeking secure software applications or for software developers who wish to reach MacOS users. As an initial matter, a software developer who wants to reach users of MacOS devices must submit her applications to Apple for review and approval to be listed on the MacOS App Store. This is because Apple has designed MacOS as an increasingly closed system, including software designed to block applications not downloaded from the MacOS App Store, in order to maintain complete control over the MacOS software market.

142. For example, Apple's MacOS operating system now includes so-called "Gatekeeper" software designed to block software not downloaded through the MacOS App Store, unless consumers ignore ominous "security warnings" that Apple issues to users, or alter complex security settings on their device. Users are strongly disincentivized from running software that Apple indicates may be harmful for their computer. Thus, software applications downloaded from the Internet, and subject to active security warnings from Apple, are not reasonable substitutes for software applications downloaded through the MacOS App Store, and using the Internet as a channel of direct distribution is not a reasonable substitute for distributing software through the MacOS App Store, because Apple's own software separates these two channels into separate software markets with separate security implications for users.

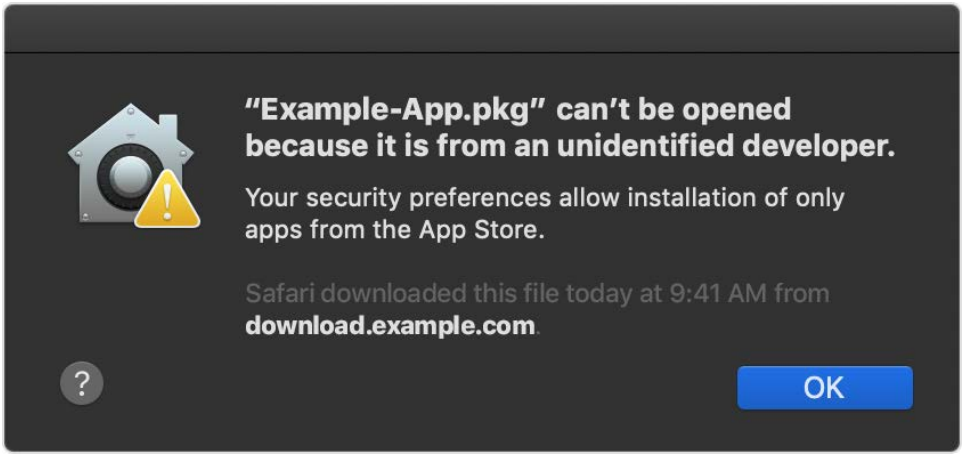
143. Apple documentation confirms that software applications downloaded from the Internet are not a reasonable substitute for software applications downloaded through the MacOS App Store, as Apple actively warns users against downloading and installing applications in this fashion.

144. Apple explicitly tells consumers that downloading applications from the App Store is the only secure way to receive applications, and that Internet downloads are not reasonable substitutes for App Store-approved applications: "The safest place to get apps for your Mac is the App Store… macOS includes a technology called Gatekeeper, that's designed to ensure that only trusted software runs on your Mac… By default, the security and privacy preferences of your Mac are set to allow apps from the App Store and identified developers. For additional security, you can choose to allow only apps from the App Store."[16]

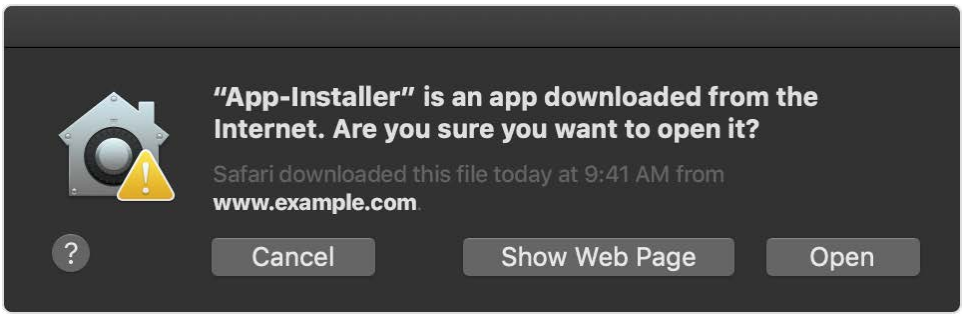
145. Apple's MacOS operating system includes so-called "Gatekeeper" software designed to block software not downloaded through the MacOS App Store, unless consumers affirmatively choose to allow software that Apple ominously warns users may not be safe.

146. Using Apple's recommended settings for "additional security" by "choos[ing] to allow only apps from the App Store" (Ex. 11), a MacOS user is prohibited from downloading and installing applications through any means other than the App Store:

[16] *See* Ex. 11, "Safely open apps on your Mac," https://support.apple.com/en-us/HT202491.



147. Even if users ignore Apple's suggested settings for "additional security" (Ex. 11) and opt to allow for installation of software installations received outside the MacOS App Store, Apple further discourages users from installing applications once downloaded, displaying ominous warning messages designed to discourage users from running those applications:



148. Apple's security documentation for users discourages users from accepting software when this warning is displayed: "You may want to look for a later version of the app in the App Store or look for an alternative app."

149. Apple's MacOS security settings for applications, including its Gatekeeper software, are designed to further Apple's strategy to ensure users face significant barriers when attempting to download MacOS software applications through any source other than Apple's MacOS App Store. Apple warns MacOS users that no method of application delivery is a reasonable substitute for the App Store, saying that the MacOS App Store should be sole trusted

source of applications: "The safest place to get apps for your Mac is the App Store… Apple reviews each app in the App Store before it's accepted and signs it to ensure that it hasn't been tampered with or altered." Ex. 11.

150. On information and belief, given Apple's security warnings and admonishments to consumers, and Apple's Gatekeeper software designed to exclude MacOS applications obtained from sources other than the MacOS App Store, the majority of users do not and cannot obtain MacOS applications except through the MacOS App Store. Indeed, a significant portion of users are unwilling to disregard Apple's security warnings and download and install applications Apple flags as allegedly unsafe, as compared to MacOS App Store downloads.

151. User's desire for security, including for secure MacOS applications, is substantially price-inelastic. Small increases in price for MacOS App Store downloads will not cause reasonable consumers to jeopardize the security of their much more expensive Apple computers, which typically sell for thousands of dollars.

152. All of these developments—which have been the result of a concerted effort by Apple to gain ever more control over the applications on MacOS—have given Apple massive power over MacOS applications. This has, in turn, given Apple monopoly power over MacOS applications by giving it the power to determine pricing for MacOS applications and by limiting output (by acting as the gatekeeper for MacOS apps).

Apple's MacOS Monopolization: The MacOS Email Client Relevant Market

153. As discussed above, an email client is a software application used to send and receive electronic mail. Email clients are local software packages that offer a collection of features designed to facilitate sending, receiving, composing, and organizing email. These local software programs differ from command-line interfaces or from web-based interfaces, which

offer a more limited set of features and typically cannot operate locally when a device is not online.

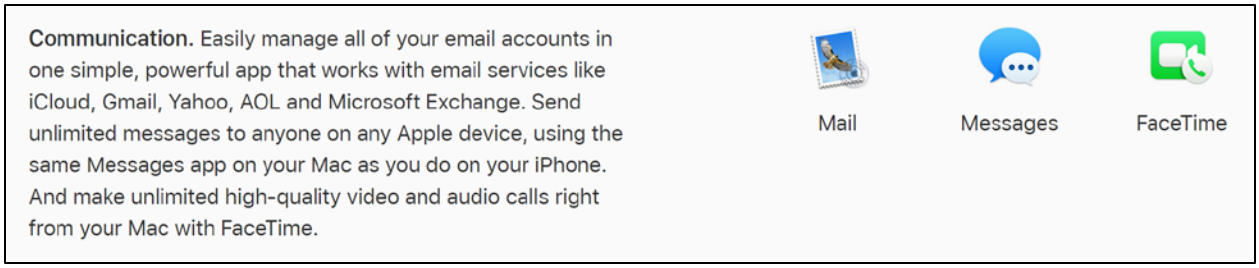
154. Mail clients are software applications designed to run on a specific operating system, such as Windows or MacOS. Email clients designed to run on one operating system (such as Windows) are not substitutes for email clients designed to run on another operating system (such as MacOS), since a software package designed to execute on one operating system will not execute on another operating system.

155. Mail clients have a unique purpose vis-à-vis other types of apps: to provide users with the ability to draft, send, and receive emails. Although other types of messaging apps and programs allow users to send and receive messages to each other, those types of messages (*e.g.*, text messages, social media messages) serve different purposes and are used in different ways by consumers. Particularly for enterprise users, mail clients are considered a "must have" app for messaging *in addition to* any other types of messaging apps.

156. The geographic scope of the MacOS Email Client Market is national.

157. The existence of email clients for operating systems other than MacOS is irrelevant to the analysis of the relevant market at issue; software developed for other operating systems is not compatible with MacOS devices, and therefore those applications are not reasonably interchangeable substitutes for MacOS email clients.

158. Apple pre-installs its own email client, Apple Mail, on all MacOS devices. Apple encourages MacOS users to use this "simple, powerful app that works with email services like iCloud, Gmail, Yahoo, AOL and Microsoft Exchange."



See Ex. 12, https://www.apple.com/ca/macos/what-is/.

159. By pre-installing Apple Mail on all MacOS devices, Apple has long enjoyed a dominant position in the MacOS Email Client Market. Apple's "Apple Mail" application is installed as the default email client for all 100 million MacOS users.

160. Apple's dominance in the MacOS Email Client Market is threatened by competition from innovative entrants, liks BlueMail, that provide a more appealing user experience through a cutting-edge design and a more attractive blend of features to users—including innovative messaging features not available through Apple Mail. BlueMail's anonymous email features compete directly with Apple's aspirations in this area.

161. Apple has given users the illusion of choice in the MacOC Email Client Market while simultaneously taking steps to foreclose competition in that market. This includes Apple's elimination of BlueMail for MacOS from the MacOS App Store.

162. As one example of Apple's effort to foreclose competition, on information and belief, Apple intentionally decided to promote low-quality competitors, to give consumers the illusion that only low-quality applications were available as substitutes for Apple's pre-installed Mail application.

163. For example, in or about July 2019, Apple chose to promote "Airmail Zero," listing the application under "Apps and Games We Love Right Now." But the application was rated below 2.0 by users, displaying a "1.7 out of 5" user rating under "Ratings and Reviews."

164. On information and belief, Apple has also artificially inflated demand for its software offerings by misappropriating technology from rivals. One example of this is Apple's misappropriation of the patented features of the '284 patent. The patented features in the '284 patent, employed by BlueMail, are highly attractive to end-users. Apple admitted during its 2019 Worldwide Developers Conference that these anonymous communication features solved a pressing problem Apple and many other software developers wanted to solve, to address end-user concerns and meet market demands: electronic communication "can be convenient, but it also can come at the cost of your privacy. Your personal information sometimes gets shared behind the scenes and these log ins can be used to track you. We wanted to solve this and many developers do too." Ex. 4.

165. In addition to more appealing user experiences, Apple's dominance in the MacOS Email Client market, as well as its Mac computer sales generally, are threatened by cross-platform messaging solutions, such as BlueMail. If a user is able to use a consistent mail client across different operating systems and platforms, then that lowers their switching costs and decreases their incentives to stick with the same operating system/platform they used before. This broadening of choice is anathema to Apple's closed garden approach and its desire to keep switching costs as high as possible, so users are locked into its devices.

Apple's Monopolization: Eliminating Competition, Including BlueMail

166. On April 6, 2019, BlueMail—which was already wildly popular on Android, and trying to gain similar success on iOS—was uploaded to Apple as an application on the MacOS App Store. BlueMail was in Beta testing at that time. This timeframe allowed Apple to better understand BlueMail's targets.

167. BlueMail was submitted for Apple's approval.

168. On May 8, 2019, BlueMail was published to the MacOS App Store and made available for public download.

169. BlueMail was a rapid success in the MacOS App Store. In only a few weeks, BlueMail was one of the top-ranked email clients for MacOS.

170. Shortly after Apple witnessed BlueMail's rapid success in the MacOS Email Client Market, Apple suddenly questioned its own decision to publish BlueMail in the MacOS App Store.

171. On May 21, 2019, Apple suddenly and spontaneously claimed that "Upon re-evaluation, we found that your app is not in compliance with the App Store Review Guidelines." Specifically, Apple claimed that BlueMail violated "Guideline 4.3 – Design – Spam" because, according to Apple, "This app duplicates the content and functionality of other apps submitted by you or another developer to the App Store, which is considered a form of spam." Apple threatened to remove BlueMail if "an update compliant with the App Store Review Guidelines" was not received "within 48 hours."

172. Apple's claim that BlueMail violated "Guideline 4.3" for "Spam," after BlueMail had initially been approved, released, and grown popular with users, was facially absurd. Apple's "Guideline 4.3" states: "4.3 Spam. Don't create multiple Bundle IDs of the same app. If your app has different versions for specific locations, sports teams, universities, etc., consider submitting a single app and provide the variations using in-app purchase. Also avoid piling on to a category that is already saturated; the App Store has enough fart, burp, flashlight, and Kama Sutra apps, etc. already. Spamming the store may lead to your removal from the Developer Program."

173. Nothing about BlueMail violated Guideline 4.3. BlueMail was and is a high-quality mail client with innovative features and a clean, attractive user interface loved by users—not a "fart" or "burp" application, and not a duplicate of another application available on the App Store.

174. On May 23, BlueMail engineers uploaded a new version of the application as requested, with a new user interface (UI) design, explaining that "In this release, we have changed the UI and think the app is unique in its capabilities, as well as its design. If you still think the app is too similar to others, can you please elaborate on which apps you find similar, so we can look into it and take action if required."

175. Less than two hours later, on May 23, Apple again rejected BlueMail, claiming that "Your app duplicates the content and functionality of apps currently available on the App Store." Apple declined to identify which supposedly duplicative applications had triggered the rejection.

176. On June 3, Apple again rejected BlueMail again, claiming that "Your app still duplicates the content and functionality of apps currently available on the App Store."

177. On June 3, BlueMail engineers again asked Apple to explain the basis for this rejection: "Could you please let us know which app or apps do you refer to, as we believe our app is unique and have removed any similar apps from the App Store."

178. On June 4, Apple identified an allegedly-duplicate application: "Your app duplicates the content and functionality of other app submitted by another developer to the App Store, which is considered a form of spam: ***TypeApp***."

179. This June 4 email marked Apple's first reference to TypeApp—a separate mobile application developed by a separate company affiliated with Mr. Volach. TypeApp, unlike

BlueMail, targets email service providers, and is customized to the needs of those service providers. For example, TypeApp is customized for Locaweb Servicos de Internet S/A in Brazil, whereas BlueMail has no Brazil-specific customization.

180. Apple's June 4 claim that BlueMail and TypeApp were "duplicates … currently available on the App Store" was false, and a pretext for Apple's anticompetitive decision to eliminate competition from BlueMail's rapid growth. TypeApp for Mac had been voluntarily removed from the MacOS App Store weeks earlier, on May 23, 2019, and was not currently available on the App Store on June 4, 2019.

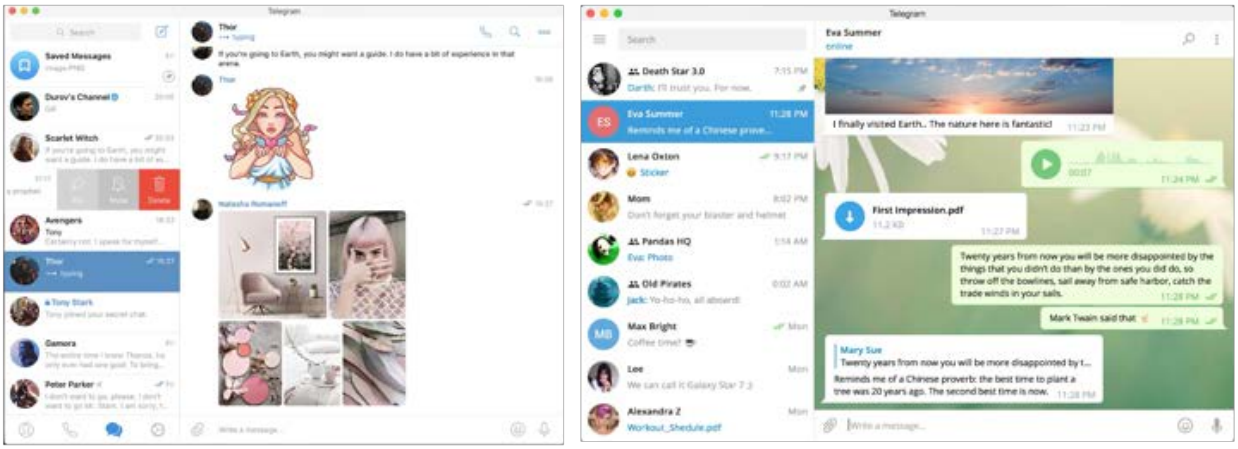
181. BlueMail and TypeApp are not duplicate applications—and they certainly could not be "duplicates" on June 4, 2019 that were "currently available on the App Store" when TypeApp for Mac had already been voluntarily removed weeks earlier and was not currently available on the App Store.

182. Apple had already approved both TypeApp and BlueMail, but said nothing for months regarding supposed similarities between those applications – waiting until the time of Apple's patent infringement to suddenly eject BlueMail from the MacOS App Store.

183. Tellingly, Apple has not enforced Guideline 4.3 against applications that are far more similar than TypeApp and BlueMail – demonstrating that Apple's reference to Guideline 4.3 was a pretext to hide its true objectives.

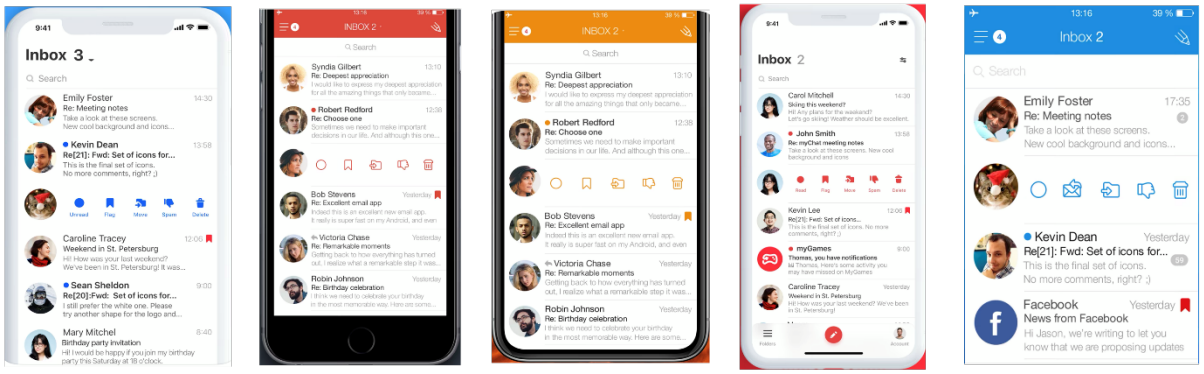
184. As one example, Telegram offers two extremely similar applications in the MacOS App Store. "Telegram" and "Telegram Desktop," both of which run on MacOS computers, and are highly similar visually:

Telegram **Telegram Desktop**



185. As another example, Apple has approved myriad email applications for the iOS App Store that are nearly visually identical, without labeling the applications as "duplicate" offerings:

Mail.ru **Mail App for Gmail** **Mail App for Hotmail** **myMail** **Mail.ru UA**



186. These are only a few examples among many. Apple's highly selective application of Guideline 4.3 demonstrates that Apple used this policy as a pretext for its decision to remove BlueMail.

187. On June 5, BlueMail engineers explained this to Apple, noting that "We just checked again the Mac App Store and TypeApp was indeed removed (Developer rejected) from

the store. This makes us a unique app. Can you please approve our latest version, or should we upload a new version?"

188. On June 5, even after the false nature of its pretextual justification for the rejection had been pointed out, Apple refused to withdraw its rejection, without explanation or apology. Apple simply stated that "After further review and consideration we have found that your application is still not in compliance with our guidelines."

189. On June 7, 2019 at 3:15am EST, days after Apple announced its infringing "Sign In With Apple" service that mimicked certain BlueMail functionality, Apple finally removed BlueMail from the MacOS App Store, without any further explanation for its conclusory June 5 claim that BlueMail was "not in compliance with our guidelines."

190. On information and belief, and based on Apple's comments regarding a policy to remove applications with features that supposedly are "duplicative" of TypeApp or BlueMail features, Apple removed other unnamed "duplicate" applications with functionality similar to the BlueMail mail client. On information and belief, this pattern of removing MacOS mail clients shields the Apple Mail email application from competition and, *inter alia*, artificially reduces consumer choice for MacOS mail clients.

191. On information and belief, Apple's removal of BlueMail under Guideline 4.3 was pretextual. At all relevant times Apple knew BlueMail was not spam, knew that BlueMail did not violate Guideline 4.3, and did not in good faith believe BlueMail was duplicative of other applications. Apple's vague rejection was part of Apple's scheme to remove competition from the App Store. On information and belief, Apple has engaged in similarly pretextual application rejections for the purpose and with the effect of maintaining a firewall from competition around Apple Mail.

192. Apple's pretextual and selective use of the App Store Guidelines is a longstanding problem. According to Techcrunch, Apple routinely enforces the App Store Guideline selectively: "Apple has written the App Store Review Guidelines, a lengthy document intended to answer all questions about what's acceptable — but those rules are not enforced consistently, and the App Store isn't a level playing field."[17]

193. Recent communications between Blix and Apple confirm that Apple's earlier rejection of BlueMail as a "duplicate" was pretextual.

194. As noted above, on June 5, 2019, the BlueMail team informed Apple that TypeApp had already been "removed" from the App Store, weeks before BlueMail was rejected under Guideline 4.3.

195. That same day, in Apple's response, Apple did *not* contest that TypeApp had been removed. Instead, Apple appeared to accept that TypeApp had been removed, but nonetheless maintained that the application was not in compliance with the Guidelines: "After further review and consideration we have found that your application is still not in compliance with our guidelines."

196. As noted above, BlueMail and TypeApp are not duplicate applications—but they certainly could not be "duplicates" on June 4, 2019 that were "currently available on the App Store" when TypeApp for Mac had already been voluntarily removed weeks earlier.

197. Nonetheless, in December 2019, after more than *six months* of silence, Apple finally contacted Blix to discuss BlueMail's removal. This was Apple's first communication with Blix since June 2019.

[17] *See* Ex. 20, "Apple's Control Over The App Store Is No Longer Sustainable," https://techcrunch.com/2019/10/21/apples-control-over-the-app-store-is-no-longer-sustainable/.

198. In that December 2019 discussion, for the first time in six months, Apple suddenly claimed TypeApp had *not* been removed from the App Store. In a series of shifting explanations, Apple claimed (1) that the "remove" option did not actually remove an application; (2) that another user account would be needed to actually remove TypeApp; and (3) that an "archive" button needed to be pressed in order to remove TypeApp.

199. These shifting explanations were themselves not credible, and at times internally inconsistent. A developer removing their application from the App Store would, Apple acknowledged, remove the application from sale –making it unavailable, rather than "currently available on the App Store," as Apple claimed when rejecting BlueMail.

200. Moreover, Apple's statements in December 2019 confirmed its removal of BlueMail as a "duplicate" must have been pretextual, because Apple employees stated in December 2019 that Apple *could not even run TypeApp or BlueMail*. According to Apple employees, Apple's App Store review team was unable to run either application in MacOS Catalina. Apple claimed this was an independent Guideline violation and that Apple thus could not evaluate the applications. But if Apple could not run the applications, Apple of course could not fairly conclude that the applications were duplicates.

201. On information and belief, Apple's shifting explanations in December 2019 for its rejection of BlueMail were a litigation-inspired effort to cover Apple's tracks. Apple's new claim that the "remove" feature it offers developers does not actually remove a developer's application is not plausible; users cannot download a developer-removed application. Moreover, its claim that TypeApp was not actually removed from the App Store is not consistent with TypeApp's "removed (developer rejected)" status, which Apple admits makes the application unavailable for purchase on the App Store. Apple's December 2019 claims are also inconsistent

with Apple's May and June 2019 allegation that BlueMail supposedly "duplicates the content and functionality of apps *currently available on the App Store*," when TypeApp indisputably was *not* available on the App Store. Finally, Apple's silence speaks volumes: for six months, Apple made no claim that TypeApp had not been removed from the App Store, and did not contest this point from June 2019 (when the BlueMail team expressly informed Apple it believed TypeApp was already removed) until months after litigation had commenced.

202. Apple's removal of BlueMail from the App Store causes severe damage to BlueMail – as Apple knew it would. In the words of an ex-Apple employee, published in May 2019 by Bloomberg, Apple knows its App Store removal and rejection decisions "are what's stopping an app from getting on the store and potentially making money for this developer to put food on the table and send their kids to school. It broke my heart every time I had to make those calls." [18]

203. By reducing competition in the MacOS Email Client Market, Apple harmed innovation. MacOS software developers have little to no incentives to create new software with new features and new functionality if they cannot recoup their investments in research and development by actually distributing their software and reaching users. Apple's decision to block access to the MacOS App Store based on vague claims of duplicate "features and content" discourages entry in the MacOS email client market, and disincentivizes the creation of competing software products in that market.

204. According to Apple's announcements, "Sign In With Apple" will be available on all platforms, accessible for everyone on the Internet, including Windows and Android. Apple

[18] *See* Ex. 21, "Inside the Apple Team That Decides Which Apps Get on iPhones," https://www.bloomberg.com/news/articles/2019-05-28/why-did-apple-reject-my-app-ex-head-of-app-store-review-explains.

has realized the crucial importance of cross-platform availability and has specifically advertised cross-platform availability of the "Sign In With Apple" service: "Sign In with Apple is cross-platform. The API is available on all Apple platforms: iOS, MacOS, WatchOS, tvOS. The sign-in experience is tailored on each platform for ease of use. The JavaScript API enables you to use Sign In with Apple on the web as well as other platforms like Windows or Android."[19]

205. "Sign In With Apple"—and particularly, its infringing features for anonymous communication—appears to be a critical component of Apple's plans for the future of messaging. Apple's own CEO explained that Apple is betting heavily on this feature and its anonymous communication features, explaining in public comments (which were made just before Apple dropped BlueMail for Mac from the App Store) on June 3rd, 2019: "We are pushing forward and I hope that everyone that wants to not be surveilled across the Internet, I hope they use our Sign In."[20] Put simply, Apple saw the threat BlueMail and other cross-platform messaging solutions represented to its mail client's and computers' competitive standing, and took steps to thwart that competition based on the monopoly power it enjoys over MacOS applications.

COUNT I

Infringement of the '284 Patent

206. The allegations in the preceding paragraphs are incorporated by reference as if fully set forth herein.

[19] A video of this presentation is available online at https://developer.apple.com/videos/play/wwdc2019/706/. An excerpt from Apple's transcript of that presentation, taken from the same website, is attached. *See* Ex. 5.

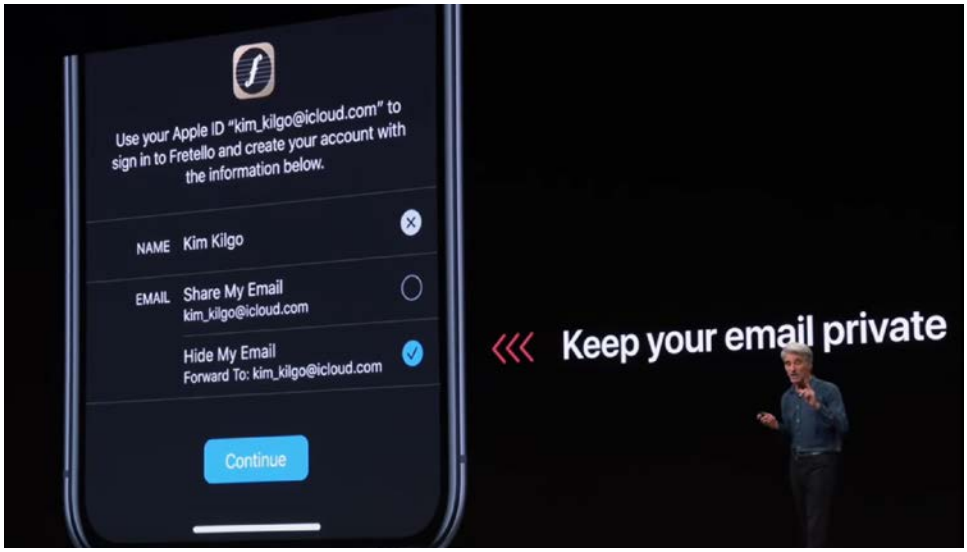
[20] *See* Ex. 13, Tim Cook interview with Norah O'Donnell (CBS News, June 3, 2019), https://www.cbsnews.com/video/tim-cook-on-immigration-tariffs-and-spending-too-much-time-on-our-phones/.

207. As explained herein, and on information and belief, Apple has directly infringed, and continues to directly infringe, at least claims 1-5, 7-10, 12-13, 17-18, 21-22, 26-30, 33-34, and 36-37 of the ’284 patent by making, using, offering for sale, selling, and/or importing into the United States the infringing “Sign In With Apple” system, including iOS devices with an API specifically configured to perform infringing operations, and has contributed to and/or induced infringement of the ’284 patent by others, including software developers and end-users.

208. For example, and without limitation, on information and belief the “Sign In With Apple” system meets every limitation of at least claims 17 and 26 of the ’284 patent, and Apple’s making, using, offering for sale, selling, and/or importing the “Sign In With Apple” system, including iOS devices running iOS 13, and Apple’s distribution of iOS 13 to such devices, directly infringes claim 1 of the ’284 patent under 35 U.S.C. § 271(a).

209. The “Sign In With Apple” system, including Apple devices specifically configured to work with that system, perform a method of controlled pre-interaction between a first party and at least one second party. For example, a first party, such as an end-user of an Apple device, and at least one second party, such as an application developer, can perform controlled pre-interaction, such as operations performed prior to communications between the end-user and the application developer, to ensure that subsequent communications via private relay will not inform the application developer of the end user’s private email address. Apple documentation confirms “Apple’s private email relay lets users receive email even if they prefer to keep their address private.” Ex. 7 Moreover, “Sign In With Apple” will also perform controlled pre-interaction operations for at least login and authentication purposes; when using the “Sign In With Apple” system, “you are authenticated with Face ID on your device, logged in with a new account without revealing any new personal information.” Ex. 4.

210. The "Sign In With Apple" system, including Apple devices specifically configured to work with that system, provides at least one private interaction address of said first party. For example, Apple presents to a first party, such as an end-user of an Apple device, at least one private interaction address of that end-user, such as an email address. Apple provides this email address to users upon sign-in via an interface asking users if they wish to "Share My Email" or "Hide My Email," as shown below:



See also Ex. 4.

211. The "Sign In With Apple" system, including Apple devices specifically configured to work with that system, defines at least one manageable public interaction address for said first party. For example, Apple defines a random email address for an end-user who selects the "Hide My Email" option. *See* Ex. 4; Ex. 5. This email address is designed to be manageable, and can be disabled at any time by an end-user: "we give each app a unique random address. This means you can disable any one of them at any time when you are tired of hearing from that app. It's really great." Ex. 4.

212. The "Sign In With Apple" system, including Apple devices specifically configured to work with that system, forms a record, wherein said manageable public interaction

address is associated with said private interaction address for said first party. For example, when the random email address receives an email from a specific application developer, Apple forwards that email to the end-user's private email address. On information and belief, Apple forwards these messages using records that associate the random email address with the user's private email address.

213. The "Sign In With Apple" system, including Apple devices specifically configured to work with that system, generates a reverse list, wherein an interaction address of said second party is associated at least with said manageable public interaction address of said first party. For example, the interaction address of an application developer is associated with an end-user's random address when the "Hide My Email" option is selected. Apple associates each random email address with one specific application developer: "we give each app a unique random address. This means you can disable any one of them at any time when you are tired of hearing from that app. It's really great." Ex. 4.

214. The "Sign In With Apple" system, including Apple devices specifically configured to work with that system, performs at least one pre-interaction act, said pre-interaction act comprises accessing said reverse list, and identifying said interaction address of said second party in said reverse list. For example, on information and belief, Apple accesses a reverse list to identify the email address of an application developer before forwarding email to that application developer via its private relay service.

215. The "Sign In With Apple" system, including Apple devices specifically configured to work with that system, determines that said manageable public interaction address of said first party is associated, at said reverse list, with said interaction address of said second party. For example, on information and belief, the "Sign In With Apple" private relay system

determines that a randomly-generated email address associated with an end-user is also associated with an application developer, at least in order to ensure that communications to the randomly-generated email address are only forwarded to the end-user if they are received from the application developer.

216. The "Sign In With Apple" system, including Apple devices specifically configured to work with that system, performs a method wherein said interaction address of said second party is obtainable from a third party or external services provider, wherein at least one reverse list entry is formed by synchronizing said interaction address of said second party with said manageable public interaction address. For example, on information and belief, Apple's "Sign In With Apple" service allows application developers to register email addresses that are obtainable from third parties and external services providers, including obtainable from Apple. Moreover, on information and belief, at least one reverse list entry in Apple's "Sign In With Apple" system is formed by synchronizing an application developer's registered email address with the randomly-assigned email address assigned for an end-user's communications with that application developer.

217. Apple's own use of Apple devices specifically configured to use the "Sign In With Apple" system and set that system in motion, including without limitation use during testing of devices such as iPhones and iPads running iOS 13, directly infringes claim 17. These infringing uses include, without limitation, Apple's testing in the United States of said devices, as well as Apple's demonstrations of the infringing method, including demonstrations to application developers, media, end-users, and to potential customers—including, on information and belief, demonstrations by Apple Store employees at the Apple Store in this District.

218. Apple's making, using, offering for sale, selling, and/or importing devices specifically configured to use the "Sign In With Apple" system and set that system in motion, including without limitation devices (such as iPhones and iPads) running iOS 13, infringes claim 26. These devices contain non-transitory computer readable media having computer-executable instructions that, when executed, perform a method of controlled reciprocating communication, as explained above with respect to claim 17.

219. Thus, the use of Apple's "Sign In With Apple" system meets every limitation of at least claim 17. Moreover, the sale of iOS devices specifically configured to use and place that system in motion infringe at least claim 26. Apple directly infringes at least those claims by offering the "Sign In With Apple" system, and devices specifically configured to place that system in motion, in violation of 35 U.S.C. § 271(a).

220. Apple has also indirectly infringed, and continues to indirectly infringe, the claims of the '284 patent by inducing infringement pursuant to 35 U.S.C. § 271(b) and/or contributing to infringement pursuant to 35 U.S.C. § 271(c).

221. On information and belief, in violation of 35 U.S.C. § 271(b), Apple specifically intended to induce infringement of the '284 patent by application developers and end-users of Apple devices, and had knowledge that the inducing acts would cause infringement, or was willfully blind to the possibility that their inducing acts would cause infringement.

222. On information and belief, Apple knew of the '284 patent since at least as early as June 2019, when Apple removed the competing BlueMail product from the App Store only days after announcing its infringing "Sign In With Apple" system. Apple has also known of the '284 patent, and of its infringement of that patent, at least since filing and service of this complaint.

223. On information and belief, Apple's customers directly infringe the '284 patent. For example, when an end-user uses the "Sign In With Apple" system in the manner intended by Apple, including for the purposes of communicating via private relay between an end-user and an application developer by way of a randomly-assigned unique email address, those activities infringe at least claim 17 of the '284 patent. Similarly, when Apple software developers use the "Sign In With Apple" system in this manner for reciprocal communications with end-users, those activities likewise infringe at least claim 17 of the '284 patent.

224. On information and belief, Apple specifically intends for end-users and application developers to directly infringe the '284 patent. Apple encourages infringement by instructing end-users and application developers by way of product support, developer documentation, and live instructional presentations that instruct users and applications developers on how to use the infringing "Sign In With Apple" system. *See, e.g.*, Exs. 4-9.

225. On information and belief, despite Apple's knowledge of the '284 patent and knowledge that end-users and application developers will necessarily infringe the '284 patent when using the "Sign In With Apple" system as instructed, Apple continues to encourage infringement.

226. Apple actively encourages application developers to create applications that use the "Sign In With Apple" service, as described herein and in Exhibits 4-9 hereto.

227. Apple's "Sign In With Apple" application programming interface (API) is specifically designed to perform the infringing functionality described herein. This API has no substantial non-infringing uses; it is designed to carry out the infringing functionality that forms the basis for Plaintiff's patent infringement claims.

228. Defendant also contributes to infringement of the ’284 patent by Apple’s end-users and application developers in violation of 35 U.S.C. §271(c). On information and belief, Apple knew of the ’284 patent since at least as early as June 2019, when it chose to eliminate an embodiment of that patent from the App Store only days after announcing its competing and infringing “Sign In With Apple” system. On information and belief, Apple offers to sell and sells within the United States devices specifically configured to operate with the “Sign In With Apple” system knowing that they constitute a material part of the claimed inventions, knowing that the “Sign In With Apple” API is especially made or especially adapted for use in infringing the ’284 patent, and knowing that the “Sign In With Apple” system is not a staple article or commodity of commerce suitable for substantial non-infringing use.

229. Apple has committed and continues to commit all of the above acts of infringement without license or authorization.

230. As a result of Apple’s infringement of the ’284 patent, Plaintiff has suffered damages and will continue to suffer damages.

231. On information and belief, Apple’s infringement of the ’284 patent has been and continues to be willful. Apple has had knowledge of BlueMail and, on information and belief, has had knowledge of the ’284 patent, since Apple decide to remove the BlueMail embodiment from the App Store days after announcing its competing and infringing “Sign In With Apple” service. On information and belief, Apple copied the ‘284 patent’s innovative disclosures, including features used in the BlueMail software, before throwing the BlueMail software application out of Apple’s App Store marketplace. Apple offered a competing system for private communication knowing the risk of infringement and/or in view of a risk of infringement that was sufficiently obvious that it should have been known to Apple. Despite this risk, Apple has

deliberately continued to infringe in a wanton, malicious, and egregious manner, with reckless disregard for Plaintiff's patent rights. Defendant's infringing actions have been and continue to be consciously wrongful, entitling Plaintiff to increased damages under 35 U.S.C. § 284.

232. Under 35 U.S.C. § 283, Plaintiff is entitled to injunctive relief precluding further infringement. Apple's wrongful conduct has caused and will continue to cause Plaintiff to suffer irreparable harm resulting from the loss of its lawful patent right to exclude others from making, using, selling, offering to sell, and/or importing Plaintiff's patented inventions. On information and belief, Apple will continue to infringe the '284 patent unless enjoined by this Court.

COUNT II

Monopolization Under 15 U.S.C. § 2 – MacOS Email

233. The allegations in the preceding paragraphs are incorporated by reference as if fully set forth herein.

234. For purposes of this claim, the relevant product market is the MacOS Email Client Market, and the relevant geographic market is the United States.

235. Apple's ability to exclude competition in the MacOS Email Client Market is direct evidence of its monopoly power.

236. Apple's own Apple Mail email client is pre-installed on 100% of end-user's MacOS machines.

237. There are no reasonably interchangeable substitutes for MacOS email clients.

238. Apple's complete control over the MacOS App Store imposes a significant barrier to entry in the market for MacOS email clients.

239. Apple illegally leveraged its monopoly power over MacOS applications, via its control over such applications' distribution, in order to maintain and extend its monopoly position in the market for MacOS email clients.

240. Apple purports to have the authority to remove any application that allegedly "duplicates" another application's features—for example, the features of Apple's own Apple Mail email client, which is already present on all MacOS computers by default – and Apple has used this authority to remove competition in the MacOS Email Client Market, including competition from BlueMail and other unnamed email clients Apple alleged were "duplicates."

241. Apple willfully maintained its monopoly power in the MacOS Email Client Market through its anticompetitive conduct described herein. In so doing, Apple inflicted substantial antitrust injury on Plaintiff in violation of the Sherman Act, § 2.

242. No competitors can enter the MacOS Email Client Market and effectively compete with Apple without access to the MacOS App Store, which Apple created and has shaped to erect significant barriers around its market power over MacOS applications.

243. Consumers do not have full information regarding their lack of choice in MacOS email client applications when they make their decision to enter the MacOS ecosystem or select a MacOS email client. Apple promises users will have choice, but is offering only the illusion of choice, while simultaneously exercising its monopoly power to restrict choice.

244. Apple abused its market power over the MacOS applications (via the MacOS App Store, which Apple created, separate from Internet distribution, and maintains through its Gatekeeper software and other software intended to exclude applications that are not Apple-approved) to protect and extend its monopoly in multiple markets, including the market for MacOS email clients.

245. Any purported procompetitive justification Apple might raise to rationalize its anticompetitive conduct fails because it is pretextual. Apple's own correspondence with BlueMail (and its pretextual claims of "duplication" with TypeApp, an app that was no longer available on the App Store) demonstrates that Apple's stated reasons for BlueMail's removal were pretextual.

246. But for Apple's unjustified actions, BlueMail would have continued its ascent as a leading MacOS email client.

247. Apple removed the threat of competition from BlueMail and other MacOS email client competitors, and precluded BlueMail and those other competitors from reaching a larger user base and obtaining user loyalty in the market, that BlueMail and those other competitors would rightfully have earned through open competition.

248. Apple's removal of BlueMail from the App Store was part of a pattern of anticompetitive behavior. Apple leverages its App Store to foreclose competitors, including by ejecting competing applications from the App Store and by using the App Store to analyze competitors' offerings and identify great ideas that Apple will then misappropriate – raising rivals' costs, and sometimes driving competing software developers out of business.

249. For example, Apple is foreclosing competition by raising rivals' costs through its theft of ideas from rivals, forcing rivals to enforce their intellectual property against Apple for its theft. Apple's competitors' must submit applications to Apple for review, which Apple will then analyze and often steal ideas from. Apple's competitors' only alternative to that process of forced analysis and theft is to develop alternative platforms for application distribution – something that is not feasible, or even technically possible, given Apple's design choices in Apple's software.

250. Consumers and software developers, including Blix, suffer from Apple's pattern of using the App Store to foreclose competition. Apple's ability to use its control of the App Store to exclude rivals, to analyze and misappropriate technology from rivals, and to displace rivals forecloses competition. That in turn reduces consumer choice, discourages third-party software developers from investing in future innovative products, and reduces competition among applications.

251. In addition, Apple has acquired control of an essential facility, which is a facility that is essential to competition in the relevant markets. In particular, Apple's MacOS App Store is an essential facility. Without access to the MacOS App Store, Blix and other competitors cannot compete in the relevant markets for MacOS software, including the market for MacOS Email Clients. In fact, without the ability to distribute innovative software such as BlueMail on the MacOS App Store, Blix and other competitors cannot participate in the relevant markets for MacOS Email Clients at all.

252. Blix cannot reasonably or practically duplicate the essential facility. Blix cannot reasonably or practically start a new App Store for MacOS software.

253. Apple has denied Blix and other competitors access to the essential facility on reasonable terms. Apple is refusing to permit Blix to distribute BlueMail, or other distinct software such as TypeApp, even if Blix provides full price for distribution of the applications or any in-app purchases (*i.e.*, Apple's full requested commission for such purchases).

254. Apple can feasibly provide Blix and other competitors with access to the essential facility. In the past Apple accepted BlueMail, TypeApp, and other Blix applications, and it could continue to do so now.

255. In this manner, Apple has also anticompetitively refused to deal with Blix and other competitors. Apple has terminated a voluntary course of dealing with Blix and other competitors (*i.e.*, distribution of their applications), showing a willingness to forsake short-term profits (*i.e.*, full price for distribution of the applications or any in-app purchases) in order to achieve an anticompetitive end (*i.e.*, its monopolization of the relevant markets).

256. Apple has used its monopoly power in one market (the market for MacOS application distribution) to attempt to obtain and/or maintain monopoly power in another market (the market for MacOS email clients).

257. Apple's conduct has had an anticompetitive effect in the relevant markets, and no procompetitive effect. At the very least, the anticompetitive effect of Apple's conduct outweighs any purported procompetitive benefit.

258. Upon information and belief, Apple's conduct has not been motivated by any legitimate business purpose. To the contrary, Apple has engaged in its anticompetitive, exclusionary, and predatory conduct with the specific intent of monopolizing the relevant markets.

259. Through its conduct, Apple has succeeded in acquiring and maintaining a monopoly in the relevant markets. To the extent its conduct is not stopped, Apple will exclude competition and then be able to increase prices and retain pricing above a competitive level in the relevant markets. Alternatively, Apple will use its monopoly power in the relevant markets to artificially increase demand for its devices, including by thwarting competition from cross-platform interoperable services that lower switching costs, reduce user demand for Apple's ecosystems, and threaten Apple's supracompetitive prices for its devices.

260. Apple's conduct has had a substantial effect on interstate and foreign commerce. As alleged herein, Apple's conduct has involved trade or commerce in the United States which has a direct, substantial, and reasonably foreseeable effect, and which gives rise to Blix's claim, on trade or commerce in the United States, including Blix's efforts to engage in such trade or commerce in the United States.

261. Blix has suffered and will suffer irreparable injury of the type that the antitrust laws were intended to prevent. As explained herein, Apple's actions substantially harm competition, discouraging entry by software developers and limiting choice for consumers. Among other things, its conduct has excluded competition by Blix (and by other developers' applications), reduced consumer choice among applications, reduced developer incentives to invest in entering the relevant markets and developing innovative applications, raised significant barriers to entry, raised rival's costs to compete, tilted the playing field in Apple's favor, made it harder for Blix and other developers to compete, artificially set and increased prices and decreased output for applications, and artificially increased demand for Apple's devices and platforms (including by excluding competition from cross-platform interoperable services that lower switching costs, reduce user demand for Apple's ecosystems, and threaten Apple's supracompetitive prices for its devices).

262. Blix has been and will be irreparably injured by the harm to competition resulting from Apple's conduct.

263. Blix has been and will be irreparably injured in its business or property as a result of Apple's conduct.

264. Apple willfully maintained its monopoly power over MacOS software applications, including MacOS mail clients, through its anticompetitive conduct described above.

In so doing, Apple inflicted substantial antitrust injury on Plaintiff in violation of § 2 of the Sherman Act and is liable to Plaintiff for damages in an amount to be determined at trial.

COUNT III

Monopolization Under 15 U.S.C. § 2 – iOS App Store

265. The allegations in the preceding paragraphs are incorporated by reference as if fully set forth herein.

266. For purposes of this claim, the relevant product market is the iOS Mail Client Market, which are only available from Apple's iOS App Store. The relevant geographic market is the United States.

267. There are no reasonably interchangeable substitutes for iOS mail clients.

268. Apple has monopoly power over iOS app distribution, by virtue of its control of the iOS App Store and its prohibition against any competing iOS app marketplaces.

269. Apple has monopoly power in the iOS Mail Client Market, based on Apple's decision to preinstall Apple's own Mail application on all iOS devices.

270. Apple's ability to exclude competition for iOS apps is direct evidence of its monopoly power over all such apps, and, in particular, relevant iOS app markets, such as the market for iOS Mail Clients.

271. Apple has used its exclusive control over the iOS App Store to promote its own default software applications, including its own Mail software for iOS, and to protect those software applications from fair competition with other iOS applications, including Plaintiff's BlueMail software. Apple has done so by, *inter alia*, suppressing discovery of its highest-quality competing apps and through a variety of other means alleged herein.

272. Apple forces users to add a valid payment method (and if expired, to enter a new one) before searching within the App Store, even when users are looking for free apps. This creates barriers to searching for competition to Apple's own applications, which are preloaded on the iOS device – applications Apple allows users to select and enjoy without entering a valid payment method.

273. Apple's complete control over the iOS App Store, and consequently the ability of application developers to distribute iOS applications, reduces output and harms competition by reducing incentives to develop iOS applications, limiting consumer choice in the market for iOS applications, increasing users' search costs when attempting to locate iOS software offerings that compete with Apple's own offerings – including Plaintiff's BlueMail software – and increasing users' monetary costs for apps they purchase from the iOS App Store.

274. Consumers do not have full information regarding their lack of choice in iOS applications, including iOS email client applications, when they make their decision to enter the iOS ecosystem or select an iOS email client. Apple promises users will have choice, but is offering only the illusion of choice, while simultaneously exercising its monopoly power to restrict choice.

275. Apple illegally used its monopoly power over iOS apps in order to maintain and extend its monopoly position in multiple markets for different types of iOS software applications, including the market for iOS Mail Clients.

276. Apple is raising rivals' costs by stealing ideas from its rivals, and forcing rivals to enforce their intellectual property against Apple for its theft. Apple's competitors' must submit applications to Apple for review, which Apple will then analyze and often steal ideas from. Apple's competitors' only alternative to that process of forced analysis and theft is to develop

alternative platforms for application distribution – something that is not feasible, or even technically possible, given Apple's design choices in Apple's software.

277. By locking users into Apple's own software offerings, and by limiting the number of competing offerings from third-party software developers, Apple artificially inflates demand for its own software offerings, locks consumers into its iOS operating system, and artificially inflates the price of its iOS devices.

278. But for Apple's unjustified actions, BlueMail would have enjoyed a substantially higher search ranking over the last several years, secured a substantially larger base of iOS users, and enjoy substantial additional profits that have now been lost.

279. Apple removed the threat of competition from BlueMail, and precluded BlueMail from reaching a larger base of iOS users, that BlueMail would rightfully have earned through fair competition.

280. Apple's suppression of BlueMail in the iOS App Store was part of a pattern of anticompetitive behavior. Apple has long utilized its control over the iOS App Store to promote its own offerings and suppress competitive threats from other applications. Apple leverages the iOS App Store to foreclose competitors through a variety of means, including by making competing applications difficult to locate in the App Store, ejecting competing applications from the App Store, exposing rivals (but not Apple) to negative feedback and user ratings, and by using the App Store to analyze competitors' offerings, identify great ideas that Apple will then misappropriate, and raise rivals' costs.

281. For example, Apple is foreclosing competition and raising rivals' costs by increasing search costs for consumers to find and install competing applications. Apple is likewise raising rivals' costs through its theft of ideas from rivals, forcing rivals to enforce their

intellectual property against Apple for its theft. Apple's competitors' must submit applications to Apple for review, which Apple will then analyze and often steal ideas from. Apple's competitors have no alternative to that process of forced analysis and theft; they cannot develop alternative platforms for iOS application distribution, because Apple's design choices prohibit any other channel of iOS application distribution.

282. Consumers and software developers, including Blix, suffer from Apple's pattern of suppressing competition in the iOS ecosystem and refusing to allow competing iOS app marketplaces to operate. Apple's pattern of promoting its own applications above all others makes it harder for software developers to reach iOS users, discourages software developers from investing in future innovative iOS software, hurts innovation, harms competition among applications, and reduces consumer choice.

283. In addition, Apple has acquired control of an essential facility, which is a facility that is essential to competition in the relevant markets. In particular, Apple's iOS App Store is an essential facility. Without access to the iOS App Store, Blix and other competitors cannot compete in the relevant markets for iOS software, including the market for iOS Email Clients. Moreover, without fair access to search results from the "Search" feature of the iOS App Store – which is itself an essential facility, and the doorway to roughly 66% of all app discovery and installation decisions – Blix cannot reach consumers or distribute its innovative software. In fact, without the ability to distribute software on fair terms and reach consumers with products such as BlueMail on the iOS App Store in response to queries for keywords such as "mail" and "email," Blix and other competitors cannot participate in the relevant markets for iOS Email Clients at all.

284. Blix cannot reasonably or practically duplicate the essential facility. Blix cannot reasonably or practically start a new App Store for iOS software.

285. Apple has denied Blix and other competitors access to the essential facility on reasonable terms. Apple is refusing to permit Blix fair access to search rankings in the iOS App Store, even if Blix agrees to provide full price for user purchases of the applications or any in-app purchases (*i.e.*, Apple's full requested commission for such purchases).

286. Apple can feasibly provide Blix and other competitors with access to the essential facility. In the past Apple did not artificially promote Apple's own applications at the expense of competitors, and Apple could continue to do so now.

287. Apple has used its monopoly power in one market (the market for iOS application distribution) to attempt to obtain and/or maintain monopoly power in another market (the market for iOS email clients).

288. Apple's conduct has had an anticompetitive effect in the relevant markets, and no procompetitive effect. At the very least, the anticompetitive effect of Apple's conduct outweighs any purported procompetitive benefit.

289. Upon information and belief, Apple's conduct has not been motivated by any legitimate business purpose. To the contrary, Apple has engaged in its anticompetitive, exclusionary, and predatory conduct with the specific intent of monopolizing the relevant markets.

290. Through its conduct, Apple has succeeded in acquiring and/or maintaining a monopoly in the relevant markets. To the extent its conduct is not stopped, Apple will exclude competition and then be able to increase prices and/or retain pricing above a competitive level in the relevant markets. Alternatively, Apple will use its monopoly power in the relevant markets

to artificially increase demand for its devices, including by thwarting competition from cross-platform interoperable services that lower switching costs, reduce user demand for Apple's ecosystems, and threaten Apple's supracompetitive prices for its devices.

291. Apple's conduct has had a substantial effect on interstate and foreign commerce. As alleged herein, Apple's conduct has involved trade or commerce in the United States which has a direct, substantial, and reasonably foreseeable effect, and which gives rise to Blix's claim, on trade or commerce in the United States, including Blix's efforts to engage in such trade or commerce in the United States.

292. Blix has suffered and will suffer irreparable injury of the type that the antitrust laws were intended to prevent. As explained herein, Apple's actions substantially harm competition, discouraging entry by software developers and limiting choice for consumers. Software developers, including Blix, and consumers suffer from Apple's pattern of suppressing competition in the iOS ecosystem and refusing to allow competing iOS app marketplaces to operate. Among other things, Apple's conduct has foreclosed fair competition by Blix (and other developers' applications) by promoting Apple's own applications above all others and increasing costs for rivals, including increased search costs when consumers attempt to locate rivals, and the asymmetrical costs of exposing rivals (but not Apple) to negative ratings and user reviews in the iOS App Store. These and other acts described herein harm competition by making it harder for software developers to reach iOS users, discouraging software developers from investing in future innovative iOS software, hurting innovation, reducing competition among applications, and eliminating consumer choice. Moreover, by manipulating search results and artificially inflating demand for Apple's own software offerings and platforms over cross-platform competitors, Apple artificially increases demand for Apple's own ecosystem. This allows Apple

to artificially set and increase prices for Apple's devices and software offerings, and discourages competition from cross-platform interoperable services that lower switching costs, reduce demand for Apple's ecosystems, and threaten Apple's supracompetitive prices for devices and software offerings.

293. Blix has been and will be irreparably injured by the harm to competition resulting from Apple's conduct.

294. Blix has been and will be irreparably injured in its business or property as a result of Apple's conduct.

295. Apple willfully maintained its monopoly power over iOS software applications, including iOS mail clients, through its anticompetitive conduct described above. In so doing, Apple inflicted substantial antitrust injury on Plaintiff in violation of § 2 of the Sherman Act and is liable to Plaintiff for damages in an amount to be determined at trial.

JURY DEMAND

296. Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff respectfully demands a trial by jury of all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff requests that judgment be entered in favor of Plaintiff and against Apple as follows:

a. A judgment that the '284 Patent is directly and indirectly infringed by Apple's offers to sell, sales of, and uses of the "Sign In With Apple" system within the United States, or importation into the United States of products, including without limitation iOS products and other products using the "Sign In With Apple" API, that practice one or more of the inventions claimed in the '284 Patent;

b. A judgment that Apple's conduct, as alleged, is unlawful under § 2 of the Sherman Act;

c. An order preliminary and permanently enjoining Apple, its affiliates and subsidiaries, and each of its officers, agents, and employees and those acting in privity or concert with them, from making, using, offering to sell, selling, importing products or systems claimed in any of the claims of the '284 Patent, and from causing or encouraging others to use, sell, offer for sale, or import products or systems that infringe any claim of the '284 Patent, until after the expiration date of the '284 Patent, including any extensions and/or additional periods of exclusivity to which Plaintiff is or may become entitled;

d. A permanent injunction prohibiting Apple from further illegal monopolization of the MacOS and iOS Email Client Markets;

e. An award of damages under 35 U.S.C. § 284 in an amount sufficient to compensate Plaintiff for its damages arising from Apple's infringement, including, but not limited to, lost profits and/or a reasonable royalty, together with pre-judgment and post-judgment interest, and costs;

f. An award of damages adequate to compensate BlueMail for Apple's illegal monopolization of the MacOS and iOS Email Client Markets, based on lost sales, lost profits, price erosion, loss of market share, or any other theory the Court finds applicable, together with pre-judgment and post-judgment interest;

g. An order awarding treble damages for willful infringement by Apple, pursuant to 35 U.S.C. 284;

h. An order awarding treble damages under 15 U.S.C. § 15;

i. An accounting and/or supplemental damages for all damages occurring after any discovery cutoff and through the Court's decision regarding the imposition of a permanent injunction;

j. A judgment declaring that this case is exceptional and awarding Plaintiff its reasonable costs and attorneys' fees pursuant to 35 U.S.C. § 285;

k. An award to Plaintiff of its reasonable attorney's fees and costs under 15 U.S.C. § 15; and

l. Such other relief as this Court or a jury may deem proper and just under the circumstances.

/s/ John W. Shaw

John W. Shaw (No. 3362)
Karen E. Keller (No. 4489)
David M. Fry (No. 5486)
SHAW KELLER LLP
I.M. Pei Building
1105 North Market Street, 12th Floor
Wilmington, DE 19801
(302) 298-0700
jshaw@shawkeller.com
kkeller@shawkeller.com
dfry@shawkeller.com
Attorneys for Plaintiff

OF COUNSEL:
Steven C. Cherny
Stephen R. Neuwirth
Patrick D. Curran
QUINN EMANUEL URQUHART & SULLIVAN, LLP
51 Madison Ave., 22nd Floor
New York, New York 10010
(212) 849-7000

Adam Wolfson
QUINN EMANUEL URQUHART & SULLIVAN, LLP
865 S Figueroa Street
Los Angeles, CA 90017
(213) 443-3000

Dated: December 20, 2019